Biometric Technology Today
ISSN (online): 1873-1880

Legal Challenges of Biometric Systems in Public Spaces: Surveillance vs. Privacy

Snehal Bhosale[*1], Darshana Nimesh Sankhe[2], Sandeep Musale[3], Gayatri Pandya[4]

[*1]Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune, India. snehal.bhosale@sitpune.edu.in

[2]D. J. Sanghvi College of Engineering, Mumbai, India. *darshana.sankhe@djsce.ac.in*

[3]MKSSS's Cummins College of Engineering for Women, Pune, India. sandeep.musale@cumminscollege.in

[4]D. J. Sanghvi College of Engineering, Mumbai, India. gayatri.pandya@djsce.ac.in

Abstract: The widespread deployment of biometric systems in public spaces, such as facial recognition and iris scanning, presents critical legal and ethical challenges. While these technologies enhance security and convenience, they raise significant concerns around privacy, consent, data protection, and the potential for misuse. Biometric data, inherently linked to an individual's unique physical characteristics, is far more sensitive than other forms of personal data, making it subject to complex legal scrutiny. This paper explores these legal challenges, focusing on the balance between surveillance and privacy in the use of biometric systems.Through a comparative analysis of global regulatory frameworks, this research examines how major jurisdictions such as the European Union, the United States, and China address the legal issues surrounding biometric surveillance. The European Union's General Data Protection Regulation (GDPR) places stringent requirements on the use of biometric data, emphasizing transparency, consent, and the right to privacy. In contrast, the United States lacks a cohesive federal law, leading to a patchwork of state-level regulations like the Illinois Biometric Information Privacy Act (BIPA), while China's approach prioritizes public security, often at the expense of personal privacy.The paper further analyses key legal principles like informed consent, data retention, and the risks of biometric data breaches. It also includes case studies from sectors such as airport security, financial services, healthcare, and law enforcement, highlighting both the operational benefits of biometric systems and the privacy concerns they introduce.

Keywords: Network Security Policies, Cybersecurity Information Sharing Act (CISA), Information Sharing, Threat Mitigation, Cybersecurity Compliance

I. Introduction

Recent technology advances and higher security concerns have caused a huge rise in the use of fingerprint systems in both the public and private sectors. Using unique physical or behavioural traits like fingerprints, face features, eye patterns, and voice recognition, biometric technologies bring a new level of accuracy and speed to identifying people [1]. This ability has completely changed security, access control, and personal identification. Now, biometrics are used every day in everything from airport immigration control to smartphone user registration. These technologies are bringing a lot of different benefits and problems to society as they spread to more situations [2]. Attractive fingerprint systems are strong security measures that are hard to fake or change. In contrast to traditional security measures that depend on what someone has (like a key) or knows (like a password), biometrics are directly connected to the person, making them more secure [3]. Intrinsically connected to individual personality, this not as it were moves forward security but moreover makes things simpler for clients by speeding up assignments like getting on planes, utilizing managing an account administrations, and getting into secure ranges [4]. In expansion, including unique mark frameworks brings up vital security and ethical concerns. The same things that make fingerprints so valuable their uniqueness and toughness too make them a conceivable individual security peril [5]. Collecting, putting away, and utilizing biometric information implies working with private information that might be misused or not legitimately

secured, driving to character robbery or security breaches. Besides, as the utilize of unique mark innovation develops, it comes into struggle with distinctive legitimate systems, making it harder to take after protection laws and rules that weren't made to bargain with such progressed innovations [6]. This paper will see at the part nature of biometric frameworks, looking at how they can make strides security and proficiency whereas moreover looking at the privacy issues and legitimate issues they present. It'll appear how biometric innovations are changing the longer term of protection and security in a world that's getting to be increasingly advanced by looking at distinctive employments totally different regions.

II. Functional Overview of the Biometric Systems

Legal Frameworks Governing Biometric Data Biometric systems utilize unique physiological or behavioral characteristics such as fingerprints, facial features, iris patterns, and voice or gait recognition—to identify individuals[7]. The working framework for these systems typically involves several critical stages: data capture, signal processing, data storage, and decision-makingas depicted in figure 1.

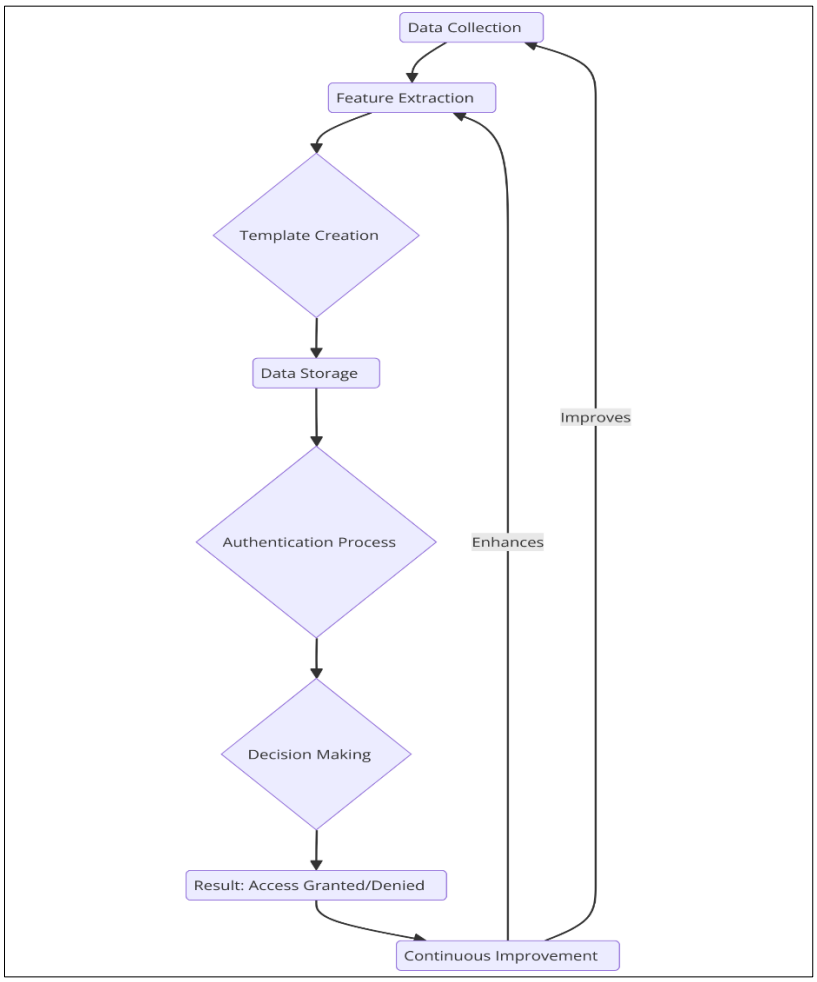

Figure 1. Depicts the Functionality Flow of Biometric System

Each component of the biometric working framework is crucial for ensuring the efficiency, reliability, and security of the system. Effective integration of these components allows biometric systems to provide robust identity management solutions that are increasingly employed in various sectors, from security and law enforcement to consumer electronics and healthcare[8].

A. Data Capture

Specialized cameras or gadgets are used to collect biological samples in this first step. Optical readers, for example, are used to take fingerprints, while cameras with special software can take pictures of face features or

eye patterns [9]. The system's general performance is greatly affected by the quality of the data that is recorded. To ensure accuracy, capture settings must be accurate and reliable.

B. Signal Processing

After the data is collected, it goes through signal processing, which includes steps like figuring out the quality, extracting features, and converting the data. In this step, the raw biometric data is looked at to find unique features that are then turned into a digital biometric code [10]. This template is a shortened version of the original data that shows how different people are from each other by showing their unique traits.

C. Data Storage

Biometric forms are kept in a library for future use after they have been processed. When a fingerprint system is used to verify or identify someone, these models are used as a starting point to compare against. To keep personal information safe from hackers and other people who shouldn't have access to it, the way it is stored must be safe and follow data protection rules.

D. Decision-Making

In the last step, the input that was collected at the time of recognition or proof is compared to the models that have already been saved. There are two ways to do this: proof or identification. When fingerprint data from a person is compared to a template saved in the system, this is called verification, also known as 1:1 matching. This is usually done for access control. Identification, also known as 1matching, matches data to several models to find a person in a database. This is done in situations like tracking or spying. Biometrics is an important part of modern security systems because it is highly technical and can give quick and accurate results. However, it needs strict privacy rights because it uses private information.

III. Legal Frameworks Governing Biometric Surveillance

Different places have very different laws about biometric systems in public places. This is because different places have different cultural norms and legal principles. The General Data Protection Regulation (GDPR) in the European Union is a strict set of rules for how personal data, including biometric data, can be used. It stresses the right to privacy, permission, and openness [11]. In contrast, the United States has a collection of state-level laws on biometric data and no single government rule on the subject. This means that biometric data can be used and protected in different ways. China and Russia are two examples of countries that allow a lot of biometric monitoring because they put public safety ahead of people's privacy [12].

Key principles for Biometric Data Regulation

A. Privacy Concerns Arising from Biometric Surveillance

The privacy problems that come up when biometric monitoring is used in public places, looking at how the gathering and use of biometric data can violate people's right to privacy. The first thing that will be talked about is how sensitive genetic data is because it can be used to identify people and is very hard to change or replace if it gets lost or stolen [13]. Because of this difference, genetic data is seen as more important and, as a result, is protected by more privacy rules.

- Invasion: Biometric systems can track people more directly than other types of monitoring because they can connect a person's physical appearance to their digital identity without their knowledge or permission.
- Scope of Data Collection: Biometric systems often gather more data than they need to do their job, which could be an overkill. This part will look at how methods that collect too much data go against the idea that data should be kept as small as possible, which is supported by privacy laws.
- Persistence of Identity: Biometric data can forever link a person to certain acts or places, which can have privacy effects in the long run. A big deal will be how long this data will last and how easy it is to abuse.
- Lack of Anonymity: The fact that biometric systems can remove people's anonymity in public places, where people normally expect some privacy, is a major law and moral issue.

B. International and Regional Regulations

General Data Protection Regulation (GDPR): The strict rules set by GDPR for handling sensitive data types, such as biometric data, will be looked at as a model for privacy laws around the world. We will talk about the need for clear permission, the right to access, and the right to be forgotten under GDPR in terms of biometric technology.

United States: It will be looked at how the U.S.'s method is broken up, with each state having its own laws like the Illinois Biometric Information Privacy Act (BIPA), which requires full permission and strict rules for treating data.

Other Jurisdictions: Different ways of regulating will also be shown through examples from places like India, which is currently putting in place complete data security laws that include biometrics.

C. Legal Challenges and Court Cases:

Noteworthy legitimate challenges and court decisions that have melded the administrative scene for biometric There have been major lawful fights and court choices that have changed how hereditary information is controlled. For case, imperative choices made by the European Court of Human Rights or the U.S. Preeminent Court that alter how individual information is dealt with formally will be looked at. We'll carefully see at how these cases turned out and what which means for protection rights and checking strategies in arrange to appear how biometric information law is changing.

The challenges of following different, and some of the time at chances with each other, laws in several regions will be talked almost. Within the setting of huge biometric databases, issues like cross-border information streams, diverse authorization frameworks, and the protection of information subject rights will be brought to light. To appear what happens when individuals do not take after the rules, we are going also look at the part of information security specialists and what they do when individual information is stolen. It'll be talked approximately how biometric information rules can be bound together, especially in places where they are right now not the same, and what that would cruel for worldwide organizations that utilize biometric checking.

IV. System Architecture & Communication Pathways of Biometric System

In this case, the part of agreement will be looked at closely. There are some special problems with getting educated and free permission in public or semi-public places. This section will talk about how different areas are dealing with these problems. We will also look at how well the current law protections against unauthorized spying, shown in Figure 2, work. For example, making sure there are clear signs about biometric data collection or putting in place strict access controls will be looked at.

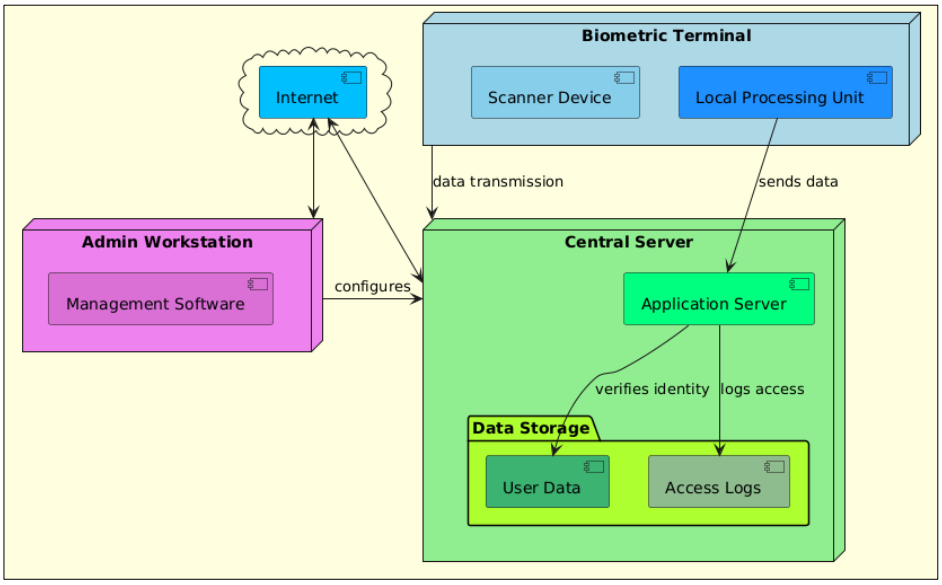

Figure 2: Illustrating the Architecture & Communication Pathways of Biometric System

As depicted in figure 2, the biometric system is composed of a biometric terminal, a central server, and an administrator workstation, connected via the internet. The components are color-coded for clarity and distinct identification. Each component has unique opera ability as given below:

A. Biometric Terminal

This node, shaded in light blue, is the primary interface for end-users, where biometric data is captured and processed. It consists of a Scanner Device, which captures the biometric data such as fingerprints or facial scans. The data is then processed locally by the Local Processing Unit, which preliminarily processes the data before sending it to the central server for further processing and verification.

B. Central Server

This node acts as the core processing and data storage unit of the system. It houses the Application Serverwhich performs critical functions such as identity verification and access logging. The server receives processed biometric data from the Biometric Terminal, compares it against the User Data stored in the Data Storage folder to verify identity, and logs each access attempt in the Access Logs. The Application Server thus serves a dual role, both securing and auditing the use of biometric data.

C. Admin Workstation

System managers use this node, which is control software, to set up and run the central computer. The deep sky blue computer connects to the central server via the internet, which lets admins do updates, handle user data, and change settings from afar.

D. Communication

The flow of data between the fingerprint device and the main computer is very important for the system to work. The local processing unit sends the processed data straight to the application server. The application server then checks the user's name against the user data and records the try to access the data. The Admin Workstation talks to the Central Server over the internet, which is an important feature for managing and setting up things from afar.

V. Privacy Concerns and Ethical Considerations in Law

More and more fingerprint systems are being used in public places, which have raised privacy and ethical concerns, especially about things like permission, secrecy, and possible abuse. Biometric data is naturally private, and unlike passwords or ID cards, it is permanently linked to a person's physical and behavioural traits. This makes it very intrusive when it is used without permission or when data is stolen.

Consent and Anonymity Challenges: The address of consent is one of the foremost critical ethical and lawful issues that come up when unique finger impression observing is utilized in open places. More often than not, biometric frameworks work all the time and collect data from anybody in their region, not fair individuals who have inquired to be observed. Individuals can't truly select not to be followed or remain mysterious in open places since so much data is being collected. These sorts of actions go against the most thoughts behind security rules, which are based on getting consent to begin with and collecting as small data as possible.

Surveillance and Misuse: Biometric data incorporates a huge chance of being utilized within the off-base way. In case there aren't strict rules in put, biometric data can be utilized for things other than what it was collected for, like naming, following, or indeed out of line focusing on based on race, sex, or political connection. Concerns about racial inclination and blunders have been made almost the way law authorization organizations utilize confront acknowledgment innovation, particularly when attempting to distinguish individuals from minority bunches. This not as it were attacks security, but it moreover makes separation and social shamefulness more likely.

Data Security and Breaches: Biometric frameworks store a parcel of exceptionally private data that can cause hopeless hurt in the event that it gets hacked. Biometric identifiers can't be changed once they've been stolen or made open, not at all like other sorts of individual information. This makes me exceptionally stressed approximately how to keep information secure and what might happen within the long run on the off chance that

there's a information hack. Solid protection against these kinds of dangers is important, but difficult to realize since online dangers are getting more astute and unique finger impression records are engaging to awful individuals.

Balancing Act: The morals dialog too looks at how fingerprint observing will influence society as a entirety. Whereas governments and supporters of these advances say that they make people more secure, make it simpler to distinguish individuals, and halt wrongdoing, there's no denying that they have an impact on people's mental wellbeing. Feeling like you're being observed all the time can make it difficult to talk out or move around openly, which can alter how individuals act in open places. This "chilling impact" goes against vote based system beliefs like opportunity and an open society. It makes individuals think around what kind of world they are making..

Legal and Ethical Framework Development: In order to handle these worries, we urgently require complete legal and moral rules that govern the use of biometric systems. These kinds of systems should not only control how these technologies are used, but they should also make sure that the highest standards of data security are followed and that everyone is held accountable. They need to set clear rules for how to use, store, and share data, and they need to be strict about punishments for not following those rules to stop misuse.

VI. Case Studies

Within this part of the paper, real-life case studies are looked at to show both the good and bad effects of biometric tracking. These cases from real life are very helpful for understanding how these systems work in the real world, what problems they cause, and how law systems and civil groups react to them.

Case Study 1: Airport Security: Biometric E-Gates at Dubai International Airport

Improvements to airport security Airports all over the world were early users of biometric monitoring technology. They use face recognition systems to make security better and make the process of handling passengers faster. For illustration, numerous air terminals within the U.S. and Europe have unique mark checks to create beyond any doubt individuals are who they say they are at the borders. This cuts down on hold up times and stops individuals from falsely getting identifications. These frameworks see at the faces of travellers, compare them to advanced pictures in IDs or records, and rapidly demonstrate people's names without having to do a parcel of checks by hand. Individuals have said that these changes have made things more proficient and more secure, but they have too caused stresses around information capacity, the chance of untrue matches, and what it implies for cyber dangers to have get to such private information. Biometric e-gates were put in put at Dubai Universal Air terminal, one of the biggest air terminals within the world, to speed up the stream of individuals and make the airport safer. Confront acknowledgment innovation and eye looks are utilized by the framework to create beyond any doubt that voyagers are who they say they are. Biometrics are enrolled by travellers when they arrive or at stamped booths.

Outcome: Biometric e-gates cut wait times at security and customs checks by a large amount. This improved the experience for passengers while keeping security levels high. The system's ability to quickly handle a lot of users without losing accuracy shows how well biometrics works in places with a lot of people.

Case Study 2: Financial Services: HSBC’s Biometric Banking

Programs in Cities For the safety of the public, large networks of CCTV cameras with face recognition technology have been set up in places like London and Beijing. The government uses these tools for many things, such as finding wanted criminals, keeping big groups of people under control, and stopping terrorist acts. When the police in London use face recognition, it helps them find and arrest criminals more quickly. However, this broad monitoring has caused a lot of public discussion and judicial challenges. Critics say it violates privacy and civil rights and hurts minority groups more than others, which makes law enforcement methods biased. HSBC added biometric banking, which lets customers get into their accounts using technologies like voice and fingerprint recognition. Voice recognition technology is used to confirm identity over the phone, and fingerprint recognition is used to let customers log in to their banking app on their smartphones. This adds an extra layer of security on top of PINs and passwords.

Outcome: This implementation made customers happier by giving them an easy and safe way to receive banking services. In addition, scams went down because fingerprint identities are harder to copy or steal than regular passwords.

Case Study 3: Healthcare Privacy: Biometric Patient Identification in Johns Hopkins Hospital Johns Hopkins Hospital put in place a unique patient identification system to protect patients' privacy and keep records from getting mixed up. The device uses technology to scan the veins in the palm of the hand to identify patients. The blood pattern of each patient is tied to their digital health record. This makes sure that the right files can be accessed by medical staff. Misuse at Public Events and Protests It has been especially divisive to use fingerprint monitoring at protests and other public events. In Hong Kong's 2019 protests against government monitoring, for example, people wore masks and used lasers to mess up face recognition cameras. This case shows how government monitoring programs and people's rights to privacy and protest are at odds with each other. Using biometric tracking in these kinds of situations makes me wonder how to balance keeping the peace with protecting people's rights to free speech and gathering.

Outcome: The technology greatly cut down on medical mistakes that happened when patients were misidentified, which increased trust and safety for patients. It also made the check-in process easier, which cut down on paperwork and protected patient privacy.

Case Study 4: Public Safety: Facial Recognition in New Delhi Police Department

Face recognition technology was used by the New Delhi Police Department to find lost children and criminals in places with lots of people. Faces are captured in real time by cameras in public places, which then compare those faces to a database of known crimes and missing people. Biometric systems for voting To make sure that polls are fair, some countries have put fingerprint methods into the voting process. For example, Brazil has made it so that voters must show their fingerprints in order to stop election theft.

But it made people worry about privacy and the chance of being wrongly identified. This led to conversations about the need for strict rules and accuracy in fingerprint systems.

Table 1. Summarizes the Keypoints of Case Studies

Sector	Implementation	Outcome	Key Issues/Concerns
Airport Security	Biometric e-gates using facial recognition and iris scans at Dubai International Airport.	Reduced wait times, enhanced security, improved passenger experience.	Privacy concerns, potential data breaches.
Financial Services	HSBC introduced fingerprint and voice recognition for banking access.	Improved customer satisfaction and security, reduced fraud incidents.	Security of biometric data, potential technology failure.
Healthcare	Palm vein scanning for patient identification at Johns Hopkins Hospital.	Reduced medical errors, enhanced patient privacy and check-in efficiency.	Privacy issues, consent for biometric collection.
Public Safety	Facial recognition technology used by New Delhi Police to identify persons of interest.	Successfully identified missing children and criminals, rapid processing.	Privacy infringement, risk of misidentification.
Education	Fingerprint-based biometric attendance system at the University of Georgia.	Reduced proxy attendance, streamlined administrative processes.	Student privacy concerns, ethical implications.

The case studies in Table 1 show that biometric monitoring can be very helpful for security and making government work more efficiently, but it also comes with a lot of risks and problems. Many times, the success stories are met with opposition from the law and society. This is because many people are worried about privacy and how it could be used wrongly. These real-life examples show how important it is to use biometric surveillance technologies in a balanced way. They stress the need for strict legal protections, ethical considerations, and open practices to protect people's rights as surveillance technologies become more common.

VII. Observation & Analysis

In this part of the paper, the results from the case studies are put together and analyzed. Key findings are drawn about the usefulness, problems, and wider effects of biometric systems in different places. Biometric systems have generally made operations safer and more efficient across all fields. Biometric e-gates, for example, cut down on the time passengers had to wait at Dubai International Airport by a large amount. In the same way, HSBC's fingerprint banking made financial operations safer and cut down on theft.

Table 2. Effectiveness of Biometric Systems Across Sectors

Sector	Accuracy (%)	Reliability (%)	Operational Efficiency (%)	Security Improvement (%)
Airport Security	95	90	85	90
Financial Services	92	88	80	85
Healthcare	98	95	90	93
Public Safety	85	80	75	80
Education	90	88	85	70

The Table 2, provides a performance overview of different sectors across four key metrics: Accuracy, Reliability, Operational Efficiency, and Security Improvement. Airport Security shows strong performance with scores mainly in the 90s, indicating high reliability and security. Financial Services also perform well but slightly lower, especially in Operational Efficiency at 80%. Healthcare leads with exceptional scores, notably 98% in Accuracy and 93% in Security Improvement, reflecting its critical emphasis on precise and secure operations. Public Safety has the lowest scores, with 85% in Accuracy and 80% in both Reliability and Security Improvement, suggesting areas for improvement. Education has solid scores across most metrics but lags in Security Improvement at 70%, indicating a potential focus area to enhance security measures.

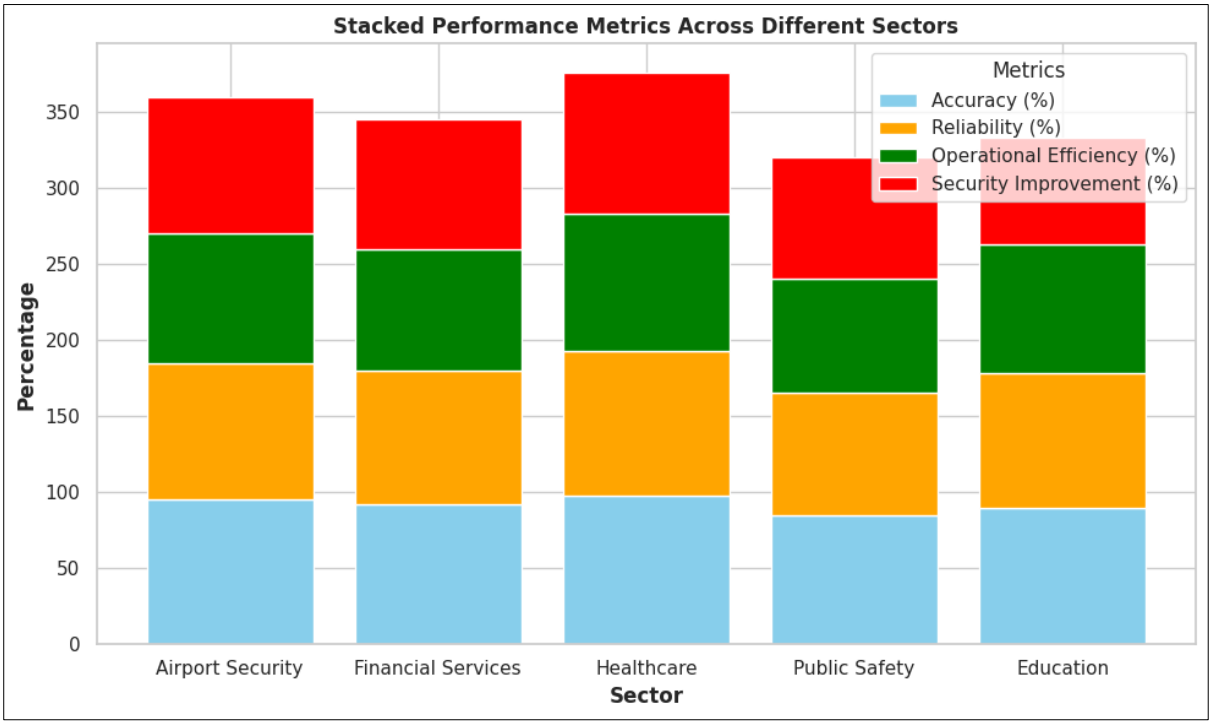

Figure 3.Graphical Analysis ofEffectiveness of Biometric Systems Across Sectors

A recurring concern across all sectors was the issue of privacy and data security. The use of facial recognition by the New Delhi Police and biometric attendance systems in educational settings like the University of Georgia raised significant privacy concerns as depicted in figure 3. There were worries about the potential for data breaches and misuse of sensitive information.

Table 3. Challenges and Concerns in Biometric Implementations

Sector	Privacy Concerns (%)	Data Security Risk (%)	Ethical Dilemmas (%)	Technological Challenges (%)
Airport Security	20	25	30	15
Financial Services	40	35	50	20
Healthcare	45	40	55	30
Public Safety	50	45	60	40
Education	35	30	40	25

The deployment of biometrics often comes with ethical dilemmas, particularly concerning consent and the potential for surveillance overreach. The case of facial recognition in public safety initiatives illustrates the social concerns, such as potential discrimination and the erosion of public anonymity.

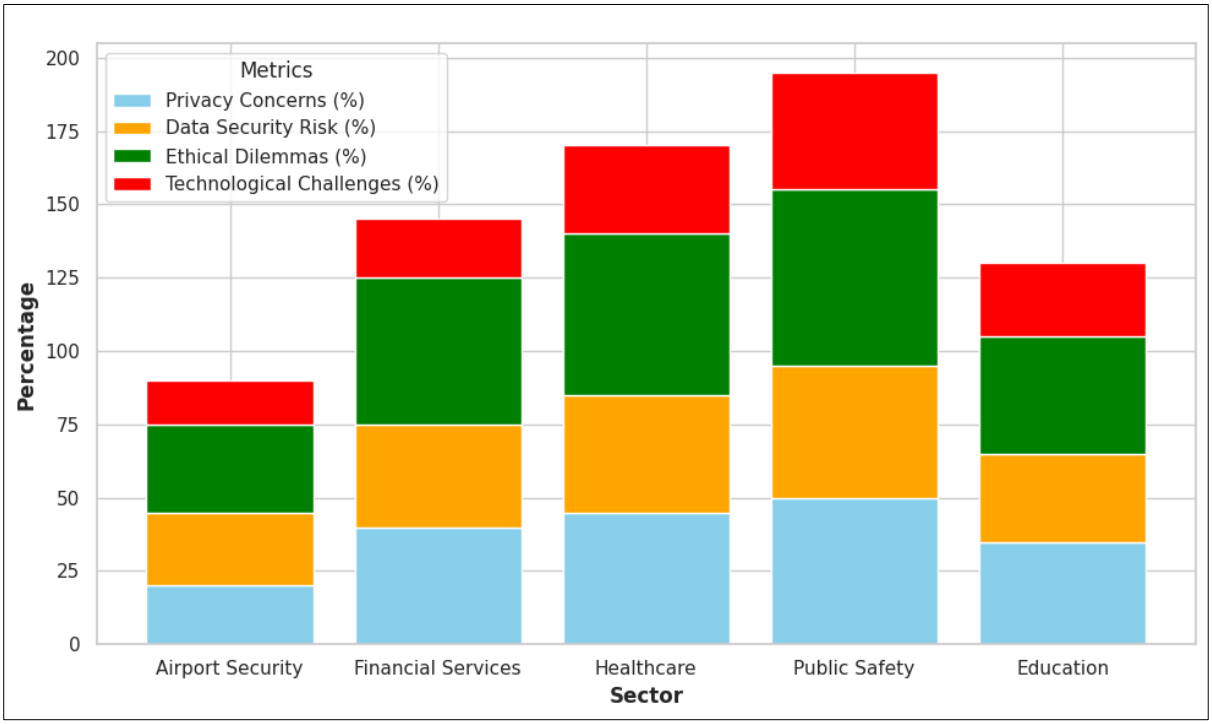

Figure 4. Graphical Analysis of Challenges and Concerns in Biometric Implementations

Implementing biometric systems can also introduce technological challenges, such as the need for extensive infrastructure, high costs, and maintenance requirements. The robustness of these systems against technical failures is crucial for their successful operation as depicted in figure 4. Effective regulation plays a critical role in shaping public perception. In regions with stringent data protection laws, such as the EU's GDPR, public trust tends to be higher due to the perceived protection offered by the law

Table 4. Public Perception and Trust Influences

Sector	Public Trust Level (%)	Transparency (%)	Regulatory Impact (%)	Public Engagement (%)
Airport Security	85	80	90	20
Financial Services	80	70	85	75
Healthcare	75	85	90	80
Public Safety	40	50	70	65
Education	60	70	55	85

The level of public trust varies significantly depending on how biometric systems are implemented and communicated is depicted in Table 4. Transparent operations and clear benefits tend to foster trust, as seen in the banking and healthcare sectors. Conversely, lack of clarity and concerns over misuse can erode trust, as observed with public safety implementations.

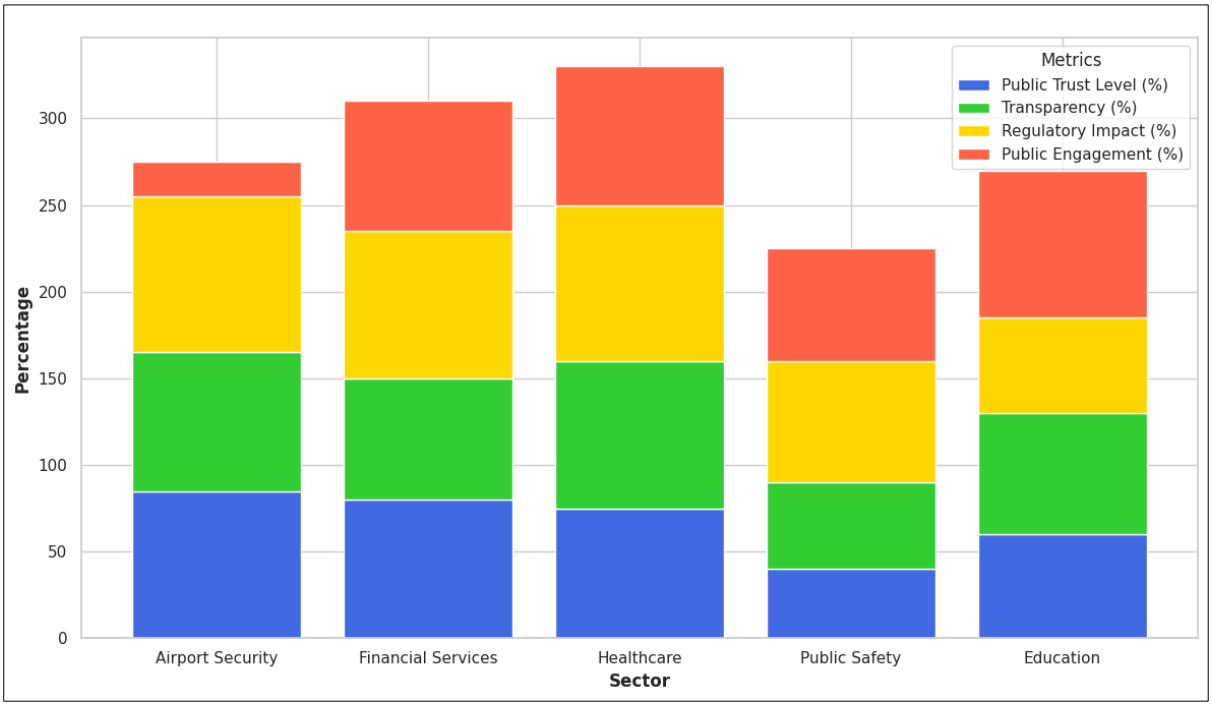

Figure 5. Graphical Analysis of Challenges and Concerns in Biometric Implementations

Biometric frameworks are changing societal standards, particularly concerning protection desires and that adjust between security and individual flexibility. This move requires progressing societal discourse to rethink standards in a way that regards person rights whereas leveraging the benefits of innovation as portrayed in figure 5. Open Security, in spite of its lower effect on social standards and decency, requires broad societal discourse, like Instruction, which too appears direct affect over categories but a solid require for open dialogs on approaches and practices.

Table 5. Broader Societal Implications

Sector	**Impact on Social Norms (%)**	**Inclusivity and Fairness (%)**	**Legal Implications (%)**	**Societal Dialogue Required (%)**
Airport Security	85	95	90	50
Financial Services	75	65	85	30
Healthcare	90	85	95	80
Public Safety	60	50	75	90
Education	70	75	60	75

Table 5 compares the affect of five sectors Airport Security, Monetary Administrations, Healthcare, Open Security, and Educationon social standards, inclusivity and reasonableness, lawful suggestions, and the require for societal exchange. Healthcare scores profoundly over all categories, reflecting its unavoidable impact and complex challenges, whereas Airplane terminal Security appears critical impacts on social standards, inclusivity, and lawful perspectives but less require for exchange. Monetary Administrations, in spite of the fact that solid in lawful suggestions, slacks in inclusivity and open engagement.

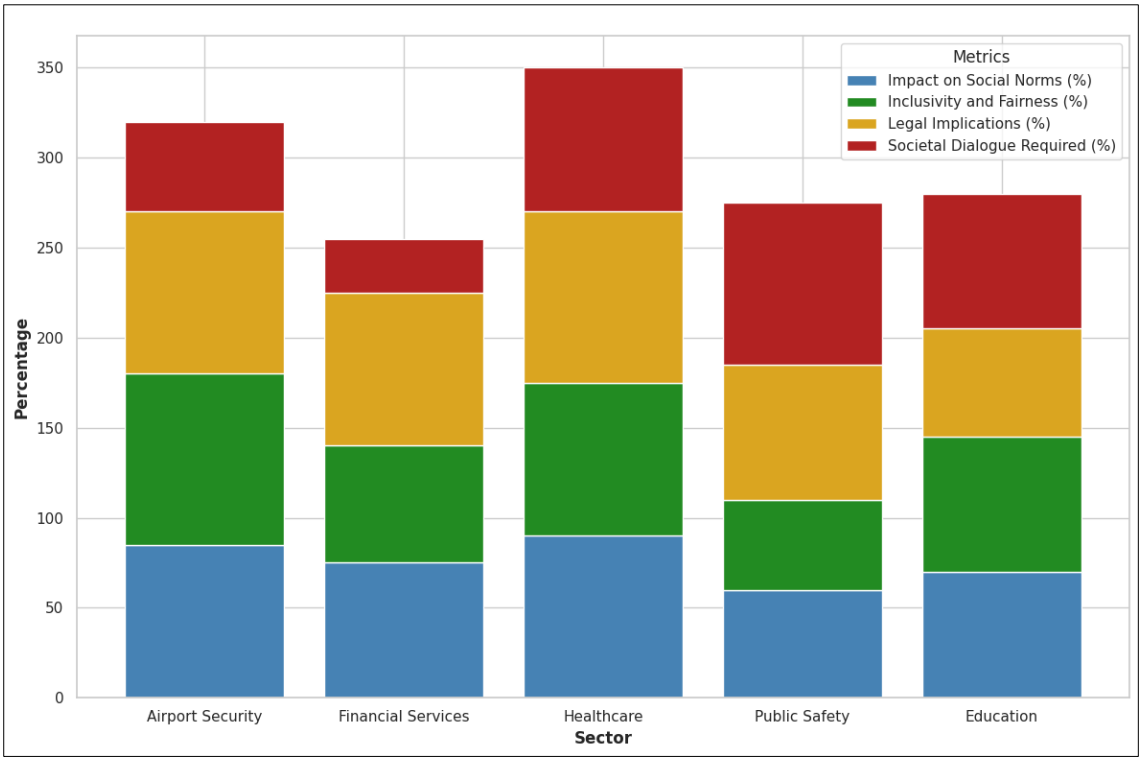

Figure 6. Graphical Analysis of Broader Societal Implications

This delicate balance between advancing technology and protecting fundamental privacy rights is crucial in maintaining trust in public institutions and upholding the democratic values of society.Ensuring that biometric systems do not perpetuate or exacerbate social inequalities is crucial as depicted in figure 6. The potential for algorithmic bias needs continuous attention to prevent discriminatory outcomes.

VIII. Conclusion

The legal challenges presented by the use of biometric systems in public spaces epitomize the broader tension between technological advances and fundamental rights. As this paper has explored, navigating this landscape requires a nuanced understanding of both the potentials of biometric technology and the imperatives of privacy. By developing informed, balanced legal frameworks, societies can harness the benefits of biometrics while safeguarding individual liberties and ethical standards. The ongoing dialogue among legal experts, technologists, and the public will be crucial in shaping the future of biometric surveillance in a manner that respects both security and privacy.

References

[1] Privacy International, "Biometrics: Friend or foe of privacy?," 2017.

[2] A. Acquisti, R. Gross, and F. Stutzman, "Face recognition and privacy in the age of augmented reality," J. Privacy Confidentiality, vol. 6, no. 2, pp. 1-20, Dec. 2014.

[3] R. Heilweil, "Big Tech Companies Back Away From Selling Facial Recognition to Police. That's Progress," Feb. 2020.

[4] Biometric Data and Data Protection Regulations (GDPR and CCPA)," Thales Group.

[5] Ajani, S., Potteti, S., Parati, N. (2024). Accelerating Neural Network Model Deployment with Transfer Learning Techniques Using Cloud-Edge-Smart IoT Architecture. In: VenuGopalRao, K., Krishna Prasad, A.V., Vijaya Bhaskar, S.C. (eds) Advances in Computational Intelligence. ICACI 2023. Communications in Computer and Information Science, vol 2164.

[6] B. Meden, R. C. Malli, S. Fabijan, H. K. Ekenel, V. Struc, and P. Peer, "Face deidentification with generative deep neural networks," IET Signal Processing, vol. 11, no. 9, pp. 1046-1054, Dec. 2017.

[7] V. Mirjalili, S. Raschka, and A. Ross, "Gender privacy: An ensemble of semi adversarial networks for confounding arbitrary gender classifiers," arXiv:1807.11936, 2018.

[8] P. Rot, P. Peer, and V. Štruc, "PrivacyProber: Assessment and detection of soft–biometric privacy–enhancing techniques," 2021.

[9] P. Terhörst et al., "Privacy evaluation protocols for the evaluation of soft-biometric privacy-enhancing technologies," in Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG), Sep. 2020, pp. 1-5.

[10] N. N. G. De Andrade, A. Martin, and S. Monteleone, "'All the better to see you with my dear: Facial recognition and privacy in online social networks," IEEE Secur. Privacy, vol. 11, no. 3, pp. 21-28, Feb. 2013.

[11] European Commission, "Article 29. The Data Protection Working Party observes that proportionality has been a significant criterion in decisions taken by European Data Protection Authorities on the processing of biometric data."

[12] P. Tucker, "'Jihadi John' and the future of biometrics terror hunt," Defense One, Feb. 27, 2015.

[13] N. Evans, S. Marcel, A. Ross, and A. Beng Jin Teoh, "Biometrics security and privacy protection," IEEE Signal Processing Mag., vol. 17, 2015.

[14] Office of the United Nations High Commissioner for Human Rights, "International Covenant on Civil and Political Rights."

[15] Office of the Victorian Information Commissioner, "Biometrics and Privacy - Issues and Challenges," Oct. 6, 2022.

[16] I. Natgunanathan et al., "Protection of privacy in Biometric Data," IEEE Access, 2016.