American Journal of Information Science and Technology
2025, Vol. 9, No. 2, pp. 128-147
https://doi.org/10.11648/j.ajist.20250902.16

Research Article

Implementing Aadhar-Linked Biometric Re-authentication Can Prevent Terrorist Misuse of India's Mobile Networks

Partha Majumdar*

Department of Computer Science, Kalinga University, Raipur, India

Abstract

In India, the escalating misuse of mobile SIM cards by terrorist groups poses a significant threat to national security. Although Aadhaar-based Know Your Customer (KYC) protocols are in place, identity verification is conducted only during the activation of the SIM card. This results in a particular vulnerability, as SIM cards can be transferred to different users without any further verification. To address this concern, this paper proposes a dynamic Aadhaar-linked biometric re-authentication framework that enables continuous verification of SIM ownership through facial recognition technology. The study details the design concepts and technical architecture of the proposed system, which combines Aadhaar's facial authentication APIs with sophisticated facial recognition models and mobile telecom networks. This framework enables regular identity verification via mobile devices, offering fallback methods like OTP verification and in-person checks for users facing biometric issues or those with limited digital access. Additionally, it incorporates adaptive verification triggers informed by user behaviour and location, striving to minimise unauthorised SIM usage in high-risk or remote regions. Implementation models based on scenarios showcase the system's adaptability in urban, rural, and border areas, reflecting the diverse connectivity and device access landscape in India. Additionally, the paper assesses the system's scalability, operational feasibility, cost considerations, and its potential for future integration with 6G infrastructure and AI-driven edge computing. Legal and ethical factors are managed by aligning with the Aadhaar Act, data protection laws, and privacy-by-design principles. The study analyses potential biases and accessibility issues, incorporating technical improvements like federated learning and liveness detection to enhance system robustness. The phased deployment strategy highlights risk-sensitive implementation and demographic inclusivity. This framework seeks to bolster India's telecom security system by shifting from static to continuous identity assurance. It enhances national security while upholding user rights and ensuring service accessibility.

Keywords

Aadhaar-based Biometric Re-authentication, SIM card Misuse Prevention, Facial Recognition Technology, Mobile Network Security, Privacy-Preserving Digital Governance

*Corresponding author: partha.majumdar@kalingauniversity.ac.in (Partha Majumdar)

Received: 23 April 2025; **Accepted:** 6 May 2025; **Published:** 6 June 2025

1. Introduction

1.1. Background and Context of the Research Problem

As national security threats evolve, the growing misuse of communication networks by terrorist organisations has increasingly alarmed governments worldwide. The widespread use of mobile communication is crucial for both the public and criminal groups. Specifically, mobile phones and SIM cards have become essential tools for terrorists, providing covert means to coordinate activities, disseminate propaganda, and evade surveillance efforts. With India facing persistent challenges from cross-border terrorism and internal insurgency, the urgency of preventing unauthorised individuals, especially foreign operatives, from exploiting the nation's telecom system has intensified. Numerous security incidents have shown that terrorists often acquire SIM cards via Indian collaborators, complicating intelligence agencies' efforts to distinguish between legitimate users and potential threats [7, 9].

In India, the telecommunications regulatory framework mandates Know Your Customer (KYC) procedures for SIM card activation. The introduction of Aadhaar, the national biometric identity system, significantly enhanced the reliability of identity verification for mobile services [20]. With over 1.3 billion residents registered, Aadhaar has created a unified and verifiable digital identity platform. Nevertheless, while Aadhaar is utilised for SIM activation, enforcement mainly occurs at the point of sale. Once a SIM card is activated using Aadhaar or another identification document, it can be transferred to another person, potentially bypassing the biometric safeguards. This loophole allows for scenarios where a terrorist might exploit a SIM card legally acquired by an Indian citizen, rendering biometric verification at the point of sale ineffective as a long-term security solution.

Current studies highlight the limitations of static identity verification and stress the growing need for dynamic, continuous, and multi-factor authentication systems in high-security settings [8, 23]. Biometric re-authentication, which necessitates users to regularly verify their identity using facial recognition or other biometric techniques, offers a promising solution to this issue. Linking the ongoing use of a SIM card to the buyer's biometric identity establishes a durable security layer, ensuring the SIM is retained by the authorised user. Importantly, advancements in facial recognition technology have significantly improved its accuracy and speed of verification through mobile cameras, even in suboptimal conditions [14, 17]. Combining this technology with Aadhaar's biometric database could enable real-time authentication through current telecom applications or government portals.

Countries around the world, including India, actively monitor and restrict the misuse of SIM cards. For instance, in 2015, Pakistan implemented biometric verification for SIM registration, requiring fingerprints to be matched with the national identity database. This initiative led to the re-verification of over 100 million SIMs and was acknowledged for improving national security [6]. Similarly, Nigeria introduced biometric registration for SIM users in 2021 in response to an increase in kidnappings and insurgent activities. These cases demonstrate that connecting biometric data to SIM usage not only mitigates criminal misuse but also enhances surveillance and enables quicker counterterrorism responses.

India's unique demographic characteristics, technological landscape, and data governance require a customised strategy. Using Aadhaar-based facial authentication for SIM verification could provide a more scalable and privacy-conscious alternative to fingerprint scanning at physical sites. Nonetheless, this system faces challenges, such as ensuring facial recognition accuracy across diverse populations, addressing insufficient digital infrastructure in rural areas, and finding a balance between user convenience and rigorous security protocols.

As terrorist methods advance and increasingly incorporate digital platforms, India must adapt its counterterrorism strategies effectively. This study evaluates the feasibility, design, and effects of implementing a biometric SIM re-authentication system using Aadhaar's digital identity framework. The goal is to assess whether such a system can effectively deter terrorists from misusing communication networks, while also considering potential operational, ethical, and legal issues. By linking static identity verification to dynamic identity management, this research seeks to suggest a technically sound and socially responsible surveillance model that bolsters national security while respecting civil liberties.

1.2. Research Question

In an era where digital communication forms the backbone of societal and economic interactions, ensuring the security of mobile networks against malicious infiltration has become a national imperative. India's telecommunications infrastructure, while technologically advanced and widely accessible, faces vulnerabilities that terrorist elements can exploit. A critical loophole lies in the transferability of SIM cards, which, despite being activated through Aadhaar-based Know Your Customer (KYC) procedures, can be handed over to other individuals, potentially allowing foreign operatives to communicate under an Indian citizen's identity. This defeats the purpose of initial biometric verification and compromises the efficacy of security protocols. The use of Aadhaar, the world's largest biometric identity system, offers a unique opportunity to extend verification beyond the point of SIM activation, enabling continuous user authentication through biometric re-verification. However, the operational feasibility, techno-

logical architecture, and socio-legal implications of such a mechanism have not been thoroughly studied.

In this context, the main research question explored by this study is: Can a biometric re-authentication system, based on Aadhaar-facilitated facial recognition, be effectively designed and put into practice to ensure that a mobile SIM card remains exclusively linked to its registered user, thus decreasing the potential for misuse by terrorist groups and enhancing national security? This question includes several guiding sub-questions. First, what is the technological feasibility of incorporating real-time facial recognition into everyday SIM usage processes, especially across the varied geographic and socioeconomic landscapes of India? Second, how can the system be crafted to reconcile the demands of national security with the constitutional rights of individual privacy and convenience? Third, what operational hurdles might arise during the implementation of such a solution by telecom operators, and what measures can be taken to address them? Lastly, what legal frameworks or regulatory changes would be necessary to facilitate the ethical application of biometric data for continuous authentication?

This research question is situated not only in the technical realm of biometric authentication and mobile communications but also within larger discussions regarding digital governance, civil liberties, and counterterrorism. Previous studies have highlighted the shortcomings of static identity checks [23], the emergence of biometric technologies as effective identification methods (Jain et al., 2020), and the successes of such policies in other nations, particularly Pakistan [6]. Nevertheless, India's socio-technical landscape brings forth distinct challenges and opportunities that require focused investigation. The findings of this study will provide a vital evaluation of whether Aadhaar-linked facial authentication for SIM card usage can act as a scalable, secure, and socially acceptable solution to prevent terrorist exploitation of communication networks.

1.3. Significance of the Research

In a world that is becoming more interconnected, where digital communication underpins modern societies, protecting mobile networks from misuse has emerged as a crucial priority for national security agencies. India, characterised by its vast and diverse population, encounters distinct challenges in managing access to telecommunication services. Although Aadhaar-based KYC norms were introduced for SIM registration, the reality on the ground shows that the authentication process is inflexible and primarily restricted to the point of sale. Once a SIM card is activated, it can be transferred to another person without additional identity checks, creating a significant security gap. This weakness has been exploited multiple times by terrorist groups, allowing foreign agents and local collaborators to communicate anonymously and thus eroding surveillance capabilities and slowing down threat detection [7, 9].

This research is significant for its timely response to a critical national issue. It examines the feasibility of using Aadhaar-linked biometric re-authentication, particularly facial recognition, to secure mobile SIM usage. The goal is to develop a robust, tamper-resistant identity verification framework. In contrast to traditional methods that depend on documentation or a one-time biometric submission, this approach introduces a model of ongoing validation, which greatly enhances the difficulty of impersonation and unauthorised access. This transition from static to dynamic identity verification aligns with the latest trends in security technology and digital governance [8, 23].

Implementing a system that requires periodic facial verification via a mobile device would have significant implications. It would not only help prevent terrorists from abusing communication networks but also improve accountability in digital transactions, particularly as mobile numbers are increasingly associated with banking, government aid, and social media accounts. Additionally, this initiative would position India as a leader in biometric security innovation, providing a blueprint for other countries facing similar issues. A global example is evident in Pakistan's biometric SIM re-verification campaign, which successfully authenticated over 100 million mobile connections through fingerprint matching with its national database, celebrated as a key achievement in counterterrorism [6]. A comparable initiative, incorporating facial recognition and Aadhaar integration, would enhance this model, providing a contactless, scalable, and advanced technological solution suited to India's digital landscape.

This research holds importance within the larger framework of civil liberties and privacy. While the enhancement of security is essential, implementing a biometric system brings forth critical questions regarding data protection, informed consent, and the boundaries of state surveillance. By addressing these concerns directly, this study adds to the ongoing conversation about ethical biometrics and responsible AI. The Aadhaar system, established by the Aadhaar Act [20], lays down a legal and operational basis for biometric identity. However, its expansion into continuous authentication must be guided by transparent governance, strong audit mechanisms, and citizen oversight. Through this study, an effort is made to find a balance between the state's legitimate need to secure its communication networks and the individual's rights to privacy and due process.

This research enhances the use of facial recognition technology in practical settings. It assesses the advantages and drawbacks of existing deep learning models like DeepFace [17] and VGGFace [14] regarding their suitability for real-world scenarios, particularly considering India's varied demographics and climatic conditions. Additionally, the study addresses the infrastructural and logistical barriers to widespread implementation, particularly in rural and low-connectivity areas, providing valuable insights for policymakers and telecom operators.

In conclusion, this study tackles a vital security gap by suggesting a biometric surveillance solution that is technologically viable, socially aware, and legally sound. Its importance reaches beyond borders, providing a framework for incorporating biometric security that honours democratic values while enabling governmental efforts to address contemporary threats. By doing so, it establishes the foundation for a secure digital India, where identity is validated not only at the outset but also continuously to ensure both public safety and the integrity of the constitution.

1.4. Overview of the Paper's Structure

This paper is structured to lead the reader through a logical examination of the significant issue of SIM card misuse within India's telecommunication system and the potential of Aadhaar-linked biometric re-authentication as a preventive solution. The organisation of the paper mirrors the journey from identifying the research problem to proposing, analysing, and evaluating a technology-driven intervention rooted in biometric security and digital governance.

The paper opens with a thorough introduction, outlining the contextual background and motivation behind the research. It emphasises the increasing exploitation of mobile networks by terrorist groups and the shortcomings of existing Know Your Customer (KYC) processes. This backdrop is bolstered by evidence from both national and international cases of SIM misuse and biometric verification systems, paving the way for a stronger solution that addresses current security gaps.

After the introduction, the research question is outlined, centring on the key issue of whether Aadhaar-based facial recognition can effectively maintain SIM ownership integrity. While the question remains broad, it is specific enough to facilitate discussions on technological feasibility, legal implications, privacy issues, and implementation hurdles.

Following this, the research section highlights the importance and timeliness of this work. It situates the research within the frameworks of global and national security, digital identity management, and the ethical implications of biometric technologies. Additionally, this section recognises that any suggested surveillance system must be technically sound and socially responsible.

The literature review offers a thorough analysis of how biometric authentication is evolving in mobile communication security, particularly examining Aadhaar-linked identity systems and their incorporation into India's telecom framework. It reviews key studies on biometric verification and looks at practical policy applications in countries like Pakistan and Nigeria. The review delves into how technologies such as facial recognition and deep learning can provide secure, scalable, and user-friendly identity verification. It also addresses legal and ethical issues associated with biometric surveillance, especially concerning India's constitutional privacy rights. Notably, the review points out a considerable research gap. Although India has the biometric infrastructure and technical capability to incorporate facial re-authentication for SIM use, insufficient policy development and empirical research are assessing how such a system could operate dynamically and fairly. Additionally, the forthcoming 6G technologies, which offer real-time AI processing and edge-based biometric computation, introduce a forward-thinking aspect to this gap, making the current research crucial and timely for enhancing the security of India's telecom industry through ongoing biometric identity verification.

The methodology section presents the conceptual and technical framework suggested in this study. It describes the integration of biometric authentication into SIM usage cycles, whether via telecom applications or centralised platforms, and explains how to implement such a system with minimal disruption for end users. Additionally, the methodology addresses system testing, performance metrics, user experience, and fallback verification mechanisms for low-connectivity or edge-case situations.

The results and discussion segments examine the anticipated outcomes of implementing this system, encompassing hypothetical situations, technical simulations, or available pilot study data. These sections investigate the possible advantages of counterterrorism initiatives, fraud prevention, and ensuring digital identity credibility. Concurrently, the discussion considers the limitations of facial recognition technology, the risks of both false positives and negatives, and the essential legal protections required to safeguard individual rights.

In conclusion, the paper synthesises key findings and emphasises its contributions to national security, technological advancement, and biometric ethics. It considers the wider implications of the proposed system and proposes avenues for future research, including the integration with AI-driven behavioural analytics or blockchain identity verification systems.

The paper's structure reflects the issue's interdisciplinary nature, combining security, technology, law, and ethics. It presents a cohesive, evidence-supported argument for using Aadhaar-linked biometric re-authentication as an effective means to safeguard India's mobile network from exploitation.

2. Literature Review

2.1. Current Landscape

The regulation and oversight of mobile communications have become crucial to global security policy frameworks today. The rising sophistication of terrorism, often marked by digitally coordinated efforts, has compelled states to adopt strong mechanisms to avert the misuse of telecommunications infrastructure. In India, the increasing occurrence of mobile phone coordination in terrorist plots has exposed a significant weakness in the identity validation process associated with SIM card usage. Although the Aadhaar-based Know Your Customer (KYC) procedure provides a strong verification system at the sale point, its one-time application leads to a

vulnerable gap. After a SIM is activated, there is no method to verify that the individual using it is the same person who originally registered it [7, 9]. This gap between identity verification at registration and actual usage represents the core challenge that this study seeks to address.

Around the world, many nations have begun adopting more dynamic, biometric-focused methods for regulating SIM cards. A prime example is Pakistan, which, through a biometric campaign in 2015, re-verified over 100 million SIMs using fingerprint authentication linked to the national identity database. This effort greatly reduced illegal SIM sales and has been recognised as a pivotal moment in enhancing the country's counterterrorism capabilities [6]. Likewise, Nigeria implemented mandatory biometric SIM registration in 2021 to address the increasing cases of violent extremism and kidnapping, showcasing how biometric measures can reinforce national security frameworks.

In India, Aadhaar serves as the cornerstone of an advanced identity management system. With biometric data from over a billion people, Aadhaar offers a centralised, trustworthy, and government-verified database that can facilitate sophisticated verification processes. However, its current use primarily limits Aadhaar verification to the service onboarding stage, such as when activating SIM cards, enrolling in welfare programs, and opening bank accounts [20]. The lack of regular re-verification poses a significant issue, particularly in high-risk sectors like telecommunications. The possibility of utilising Aadhaar for real-time or periodic biometric re-authentication, notably through facial recognition, has yet to be sufficiently explored in policy discussions or academic research.

Academic research has increasingly highlighted the drawbacks of static identity verification in our digitally mobile society. Zhou and Piramuthu (2015) advocate for multi-factor, dynamic authentication methods that respond to real-time risks and behaviours, especially in mobile and high-risk settings [23]. Their study underscores the changing threat landscape posed by mobile technologies and the necessity for adaptive verification protocols. Likewise, Jain, Ross, and Nandakumar (2020) investigate biometric systems, not just as entry-point validators but also as ongoing identity regulators [8]. Their findings indicate that regular biometric assessments can help prevent identity fraud and unauthorised access across various sectors, including healthcare, finance, and public services.

From a technological viewpoint, facial recognition has become one of the most effective and user-friendly biometric methods. Unlike fingerprint or iris scanning, facial recognition is less intrusive and well-suited for remote authentication, particularly given the widespread use of smartphone cameras. Contemporary deep learning frameworks like DeepFace [17] and VGGFace [14] have reached almost human-like verification accuracy. They are notably resilient to variations in lighting, angle, and facial expressions. These models serve as the computational foundation for scalable facial verification systems that can function effectively in real-world mobile settings.

Facial recognition technology, while promising, faces significant criticism. Issues like demographic bias, breaches of privacy, and excessive surveillance have ignited global debate. Civil society organisations and privacy advocates have voiced concerns, advocating for stricter regulations and oversight regarding the use of biometric data. In a pivotal ruling, the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) established privacy as a fundamental right, creating a constitutional responsibility for the state to ensure that any application of personal data, including biometric information, is necessary, proportionate, and supported by adequate safeguards [16].

In India's current landscape, we see a dual dynamic: while the technical infrastructure and legal framework are in place for biometric re-authentication of SIM usage, implementation is lacking. This policy gap regarding identity assurance after SIM activation has created a blind spot in India's otherwise strong digital identity ecosystem. Additionally, the rapid rise in mobile subscribers, along with the growing integration of telecom and digital services, has heightened the risks involved. Nowadays, a mobile number serves not only as a communication tool but also as a gateway to banking, healthcare, education, and governance. Unauthorised misuse of this gateway, particularly by individuals connected to terrorist or criminal organisations, could lead to far-reaching repercussions beyond the telecom sector.

In summary, the existing landscape features a partial alignment of technological readiness and regulatory aims. Although Aadhaar serves as the foundational identity system and facial recognition technology provides a scalable biometric option, the lack of dynamic identity verification for SIM usage remains a national security concern. This research is positioned precisely in the gap between potential and actualisation, as well as between surveillance and privacy. By exploring how Aadhaar-based facial recognition can be utilised for routine SIM re-authentication, the study addresses both the technological potential and the ethical duty of securing India's digital future.

2.2. Research Gap

The global security environment continues to evolve in parallel with technological innovation, yet persistent vulnerabilities remain in the way nations manage and secure identity-linked communication channels. In India, the Aadhaar system has established a foundational identity verification mechanism that is both scalable and biometrically grounded. Its integration into telecom services through KYC procedures represents a major milestone in enhancing user authentication at the time of SIM issuance. However, the singular, point-in-time nature of Aadhaar-based KYC fails to address a critical shortfall: the continuity of identity assurance throughout the lifecycle of a SIM card. Once the SIM is ac-

tivated, there is currently no mechanism in place to ensure that its usage remains restricted to the registered user. This gap becomes particularly dangerous in the context of terrorism, espionage, and other forms of organised crime, where anonymity and identity spoofing via SIM transfer or SIM cloning can easily mask the movement and communication of bad actors [7, 9].

While international precedents such as Pakistan's biometric SIM re-verification campaign have shown that large-scale biometric efforts are operationally feasible, they remain reactive. They are typically limited to one-time mass exercises [6]. Even within India, the Aadhaar system has been deployed successfully for a range of services, including welfare delivery, tax filings, and digital payments [20]. Still, its role in sustaining dynamic identity verification for telecom services remains nascent. The extant literature recognises the value of continuous or multi-point authentication to address fraud and impersonation risks [8, 23]. Still, practical implementations, particularly those integrating facial recognition with telecom systems at scale, have not been studied extensively within the Indian context.

Technologically, the advent of deep learning-based facial recognition has presented a new opportunity to operationalise low-friction, high-frequency identity checks using ubiquitous mobile devices. Algorithms such as DeepFace [17] and VGGFace [14] are now capable of verifying users with high accuracy across varied lighting and orientation conditions. However, these advancements remain largely confined to domains such as smartphone unlocking, airport security, and fintech applications. There is a notable absence of scholarly research or policy experimentation exploring the integration of such models with India's telecom regulatory framework, specifically for re-verifying SIM ownership on a periodic basis using Aadhaar-linked facial authentication.

Furthermore, a forward-looking gap in the literature pertains to how the future of mobile communication, especially with the emergence of 6G, may reshape the landscape of biometric surveillance and authentication. Expected to be deployed globally around 2030, 6G networks will offer ultra-low latency, enhanced AI integration at the edge, and the ability to support massive machine-type communication [22]. These features will be particularly conducive to deploying real-time biometric verification systems that can operate seamlessly in the background, verifying users across multiple contexts with minimal disruption. Facial recognition, iris scanning, and behavioural biometrics could all be enhanced through edge computing and AI-driven decision-making embedded in 6G infrastructure. Importantly, 6G also promises to deliver significant improvements in data security and privacy-preserving computation, opening the door for more ethically sustainable surveillance architectures.

However, while technical feasibility is growing, the regulatory, ethical, and practical dimensions remain insufficiently addressed in existing research. How can routine biometric re-authentication be designed in a way that balances national security concerns with individual privacy rights enshrined by the Indian Constitution [16]? How can telecom operators and government bodies coordinate to implement such a system without infringing upon digital freedoms or creating a chilling effect on mobile use? What are the infrastructural bottlenecks, especially in rural and remote areas, that might impede deployment?

This study positions itself at the intersection of these unresolved questions. It addresses the absence of dynamic identity verification mechanisms in India's telecom infrastructure by proposing a facial recognition-based SIM re-authentication system linked with Aadhaar. It investigates not only the technological and operational aspects of such a system but also anticipates the transformative role that next-generation communication technologies like 6G may play in scaling and securing its implementation. In doing so, the research contributes to a proactive, forward-thinking discourse on securing India's digital identity infrastructure while remaining aligned with constitutional norms and global best practices in digital governance.

2.3. Review of Related Technologies

The effective deployment of a biometric SIM re-authentication framework, especially one that incorporates Aadhaar-linked facial recognition, depends on a combination of technologies, including biometric data processing, mobile network infrastructure, secure digital identity systems, and artificial intelligence. This section examines these essential technologies, highlighting the relationship between their present capabilities and their possible use in enhancing India's national security through telecom regulation.

At the heart of this proposed solution is biometric authentication, which involves verifying individuals based on unique biological traits such as fingerprints, iris patterns, and facial features. Among these, facial recognition has gained prominence for its non-intrusive nature and scalability through widely available devices such as smartphones and webcams. Modern face recognition systems rely on deep convolutional neural networks (CNNs) to extract and compare facial embeddings. State-of-the-art architectures like DeepFace [17], FaceNet [15], and VGGFace [14] have demonstrated high levels of accuracy, often surpassing 99% verification rates in controlled environments. These systems work by mapping facial images to high-dimensional feature vectors and computing similarity scores, enabling efficient one-to-one and one-to-many matching.

Despite their accuracy in laboratory settings, real-world deployment of facial recognition systems—especially across India's diverse demographic spectrum—presents challenges in terms of consistency, bias, and reliability. Skin tone variation, lighting inconsistencies, facial obstructions, and ageing effects can influence the performance of face recognition systems. Research has shown that certain algorithms may underperform across ethnicities, leading to concerns of algo-

rithmic bias and wrongful denial of access [2]. Addressing these issues necessitates the use of demographically inclusive training datasets, robust liveness detection mechanisms, and continuous model retraining, especially when deployed in security-critical systems like telecom access control.

In the Indian context, the Aadhaar ecosystem provides a formidable platform for biometric integration. Managed by the Unique Identification Authority of India (UIDAI), Aadhaar captures and stores biometric data—fingerprints, iris scans, and photographs—for over 1.3 billion residents. It facilitates e-KYC, digital signatures, and identity verification across government and commercial services. Aadhaar's authentication framework supports both biometric and demographic checks through secure APIs, making it possible to integrate facial recognition for continuous re-authentication scenarios [20]. The use of Aadhaar Face Authentication API, introduced in 2018, provides a mechanism to verify identity using facial data in real time, a feature particularly suitable for integration into telecom applications without requiring physical presence at service centres.

On the infrastructure side, the viability of continuous biometric verification depends heavily on network bandwidth, latency, and edge computing capabilities. India's current 4G and emerging 5G networks offer improved data throughput but are still limited in terms of real-time, low-latency biometric processing at the edge. Looking ahead, the transition to 6G networks, projected for deployment by 2030, promises transformative potential. As highlighted by Wang et al. (2021), 6G is expected to support terabit-level speeds, microsecond latencies, and massive AI-driven edge intelligence [22]. These features will make it feasible to embed biometric verification algorithms into telecom edge devices, such as SIM management modules or mobile base stations, enabling passive and continuous identity assurance without the need for cloud roundtrips. AI-enhanced edge computing under 6G could support not only facial recognition but also behavioural biometrics such as voice patterns, gait analysis, or device usage fingerprints, providing a multi-modal authentication layer that is both secure and user-centric.

Security and privacy remain central concerns in biometric systems. Technologies such as differential privacy, federated learning, and homomorphic encryption are being actively explored to allow biometric data processing without compromising individual privacy. Federated learning, for instance, enables models to be trained across distributed devices without transmitting raw data to central servers, making it suitable for privacy-preserving mobile authentication. Meanwhile, liveness detection and anti-spoofing algorithms are being refined to counter threats such as deepfakes, printed masks, and video playback attacks—threat vectors particularly relevant when facial data becomes a gateway to critical services like SIM usage.

Complementing biometric technology are advancements in telecom regulation platforms. India's Department of Telecommunications (DoT) is currently rolling out the Central Equipment Identity Register (CEIR), a centralised platform to detect and block stolen or cloned mobile devices based on their IMEI numbers. This initiative reflects the state's growing capacity to track and regulate telecom access at the hardware level. However, while CEIR addresses device identity, it does not link device use to biometric user verification. Bridging this gap, by combining CEIR's device identity layer with Aadhaar's human identity framework, could yield a more integrated and secure telecom infrastructure.

Overall, the technological ecosystem required to support Aadhaar-based SIM re-authentication through facial recognition is increasingly coming into focus. From neural networks and facial recognition libraries to high-speed networks and government-regulated identity platforms, the foundational components are either already in place or rapidly evolving. What is missing is a cohesive strategy to bring these technologies together in a legally sanctioned, ethically designed, and operationally viable framework that can be scaled across India's 1.1 billion mobile subscribers.

3. Methodology

3.1. Conceptual Framework

This research is fundamentally based on the convergence of biometric identity verification, digital governance, and telecom infrastructure security. It addresses the shortcomings of the existing static Aadhaar-based KYC process. The proposal suggests a dynamic and ongoing biometric re-authentication system to reduce the misuse of SIM cards in unlawful and terrorist activities. The central premise of this framework is that identity should be revalidated over time, especially in high-risk communication channels, rather than just during the initial registration. The framework aims to fill this time gap in identity assurance by integrating real-time facial recognition with Aadhaar's biometric database, thus forming a continuous authentication loop within SIM usage behaviour.

The proposed model centres on a triadic relationship involving three main components: the individual user authenticated via Aadhaar, the telecom operator responsible for providing and managing SIM access, and the biometric authentication layer that serves as a gatekeeper among them. This model posits that once a SIM card is initially activated through Aadhaar, the user is required to periodically re-authenticate using facial recognition technology. This re-authentication can be triggered via telecom service applications or directly through device features, utilising Aadhaar's facial authentication APIs to confirm the identity of the SIM user. If verification is not completed within a specified timeframe, the SIM will be temporarily suspended until the identity is verified again.

This framework integrates elements from both surveillance security theory and dynamic identity management. According to surveillance security theory, state oversight of communication must adapt alongside evolving threat strategies [1]. In

today's environment, where digital anonymity serves as a means for subversion, static identity systems fall short. The proposed conceptual model redefines SIM identity not as a one-time credential but as a privilege that is continually validated. It encompasses recent developments in biometric computing [8], federated identity frameworks, and mobile AI applications, proposing that identity verification should be not only precise but also ongoing, resilient, and considerate of user rights.

Integrating 6G infrastructure capabilities into this framework adds a forward-thinking aspect. 6G is anticipated to offer hyper-connectivity through edge-based intelligence and real-time biometric processing, significantly improving the responsiveness and reliability of biometric verification systems. According to Wang et al. (2021), 6G will facilitate terabit-level data transfers with sub-millisecond latency, allowing biometric checks to be performed in time-sensitive or high-throughput scenarios [22]. Consequently, the proposed framework envisions a future where Aadhaar-based identity verification takes place seamlessly at the network edge, reducing user disruption while upholding stringent security standards. This intelligent edge architecture could enhance not only facial recognition but also multi-modal biometric inputs, thereby bolstering the effectiveness of SIM identity management.

To guarantee scalability and ethical alignment, the framework incorporates principles of privacy-by-design and AI governance. Privacy-by-design requires embedding user consent, data minimisation, and auditability at every stage of the system [3]. By utilising federated learning for refining facial models and employing differential privacy during the exchange of biometric data, the framework seeks to thwart centralised data exploitation and ensure compliance with privacy norms as established by the Aadhaar Act and reinforced by the Supreme Court of India's Puttaswamy judgment (2017) [16].

The framework operationally gives telecom operators the flexibility to incorporate the biometric verification module into their current service management applications. This integration provides users with a smooth app-based experience for performing periodic identity checks. Furthermore, the framework includes a fallback option—either via one-time password (OTP) delivery or physical re-verification—for users who cannot complete the facial recognition process due to technical issues or biometric discrepancies. This approach ensures inclusivity and uninterrupted access, particularly for users in rural and digitally underserved areas.

In conclusion, the framework for Aadhaar-linked biometric re-authentication combines sophisticated biometric algorithms, an expandable digital identity system, and intelligent edge telecom networks. It addresses an important security vulnerability by shifting from static identity checks to a dynamic, user-focused verification approach. Additionally, it aims to carefully balance surveillance effectiveness with constitutional rights, leading to a stronger and ethically responsible national security infrastructure.

3.2. Technical Framework

The proposed biometric SIM re-authentication system rests upon a technically cohesive and scalable architecture that integrates Aadhaar's national identity infrastructure with advanced facial recognition algorithms, telecom service delivery platforms, and secure communication protocols. The technical framework is designed to facilitate dynamic identity verification at regular intervals, using lightweight, real-time biometric checks initiated through end-user devices and authenticated via UIDAI's Aadhaar biometric database. This framework aims to transition from static registration-based access control to a fluid, continuous verification environment, adaptable across India's diverse digital infrastructure landscape.

The core of the system architecture comprises four interlinked layers: the biometric capture layer, the facial recognition engine, the telecom operator interface, and the Aadhaar authentication gateway. The biometric capture layer is implemented on the user's mobile device through the telecom operator's application or an operating-system-integrated module. This layer leverages the front-facing camera and on-device preprocessing to capture facial input, which is then encoded into feature vectors using a neural network-based facial recognition model. Existing models such as VGGFace [14], FaceNet [15], or DeepFace [17] can be adapted and trained on a demographically representative dataset to ensure fair performance across India's heterogeneous population.

To minimise latency and maximise data protection, the facial recognition engine employs an edge-computing approach, where inference can be carried out on-device, and only verification signals or encrypted biometric hashes are transmitted to the Aadhaar authentication gateway. UIDAI's Face Authentication API, introduced in 2018, serves as the central validation mechanism, enabling Aadhaar-linked matching without the need to send raw images or sensitive data over the network [20]. The use of liveness detection algorithms, such as remote blink tracking, micro-expression analysis, or thermal texture recognition, ensures that the system is robust against spoofing attacks, including those involving photographs, videos, or 3D masks.

The telecom operator interface functions as the operational mediator, integrating the facial verification layer with existing SIM lifecycle management systems. It maintains a timestamped record of successful or failed authentication attempts and determines whether a user remains in compliance with identity assurance requirements. If the verification is not completed within the defined periodic window—configurable based on risk sensitivity, user profile, or geolocation—the SIM is flagged for soft suspension. During this period, outgoing communications are restricted, and the user is prompted for biometric re-verification. Upon successful authentication, service is restored instantly, creating a

closed-loop identity validation mechanism that deters impersonation without imposing prolonged service outages.

To secure the data exchange between components, the technical architecture implements end-to-end encryption using public key infrastructure (PKI). It adheres to OAuth 2.0 for access control and tokenised session management. Furthermore, federated learning can be adopted to refine facial recognition models locally on user devices, mitigating privacy concerns by avoiding the need to centralise training data. This decentralised model update protocol allows the system to adapt to demographic shifts and ageing-related changes in facial features while preserving user confidentiality [10]. In addition, differential privacy techniques are employed to inject statistical noise into aggregate analytics, ensuring that user-specific data cannot be reverse-engineered from system logs or usage patterns.

The technical framework is future-ready by design, with built-in compatibility for 6G-enabled enhancements. As 6G networks mature, their ultra-low-latency and high-throughput capabilities will support on-device AI inference and seamless biometric interactions even in high-traffic or remote zones [22]. AI-powered decision-making at the telecom edge will further enable real-time behavioural anomaly detection, allowing the system to automatically escalate verification demands when suspicious SIM usage patterns are detected, such as SIM movement across borders, usage during surveillance blackouts, or SIM clustering within flagged locations.

Robust fallback systems also address operational resilience. For users unable to complete biometric re-authentication due to technical faults or accessibility issues, the system provisions OTP-based overrides or allows physical re-verification through authorised telecom service centres. Such redundancies are critical to maintaining service continuity and user inclusion, especially in rural regions where digital penetration remains uneven.

Finally, system monitoring is enabled via a centralised analytics dashboard used by telecom providers and regulatory authorities to track compliance metrics, authentication success rates, false match incidences, and user opt-outs. This data is anonymised and aggregated to comply with India's evolving personal data protection legislation while facilitating evidence-based policy adjustments and technological refinement.

In summary, the technical framework for Aadhaar-linked biometric SIM re-authentication integrates high-precision facial recognition with Aadhaar's secure identity verification pipeline and telecom network infrastructure. Through privacy-aware protocols, adaptive learning systems, and future-ready architecture, it offers a secure, scalable, and user-sensitive solution to address the vulnerabilities in India's current SIM usage paradigm. By anchoring the technical design in real-world telecom operations and emerging biometric standards, this framework provides a strong foundation for implementation and further innovation in the field of secure mobile identity management.

4. Solution

4.1. A System Blueprint

The proposed framework for Aadhaar-linked biometric SIM re-authentication aims to transform the identity lifecycle for mobile communication in India. Essentially, the system ensures that a mobile SIM card, activated through Aadhaar-based Know Your Customer (KYC) processes, stays consistently tied to the same individual throughout its usage. This connection is preserved not only through documentation or passive ownership records, but also through regular biometric re-authentication, mainly using facial recognition approved against the Aadhaar database. By incorporating this verification mechanism into the mobile experience, the framework effectively tackles the significant issue of SIM misuse by unauthorised individuals, especially those engaged in criminal or terrorist activities.

The system architecture consists of three main operational layers: biometric capture and validation, telecom operator coordination, and centralised authentication via Aadhaar. The biometric layer operates on the user's mobile device, utilising the front camera to capture facial scans. These scans are transformed into encrypted facial embeddings and matched in real-time using UIDAI's Face Authentication API, which has been available since 2018 and enables scalable integration into applications across both public and private sectors (UIDAI, 2017). Thanks to the effectiveness of facial recognition models such as VGGFace and DeepFace, this real-time validation is not only technically viable but also cost-effective for the computational resources available on today's mobile phones [14, 17].

To ensure scalability across India's extensive and diverse subscriber base, which boasts over 1.1 billion mobile connections as of 2024 [18], the system is designed to be modular and flexible. Telecom operators, responsible for SIM card provisioning, will incorporate biometric re-authentication modules into their self-care mobile applications or USSD-driven platforms. These interfaces will initiate routine facial verification requests at configurable intervals or upon detecting anomalies. For example, a sudden SIM transfer to a high-risk area, unexpected spikes in usage, or activity during blackout periods can trigger forced re-authentication. Every successful verification is timestamped and recorded in a secure, anonymised ledger, enabling regulatory audits while safeguarding user privacy.

Edge computing is crucial in this architecture, particularly as India moves towards 5G and eventually 6G infrastructure. With 6G's potential for sub-millisecond latency and integrated AI inference at the edge, biometric checks can occur without relying on cloud latency or data centre availability [22]. This capability not only enhances user experience through near-instant verification but also alleviates network congestion and boosts system resilience in areas with limited connectivity.

The framework is firmly built on privacy and ethical compliance. All biometric data is processed in accordance with India's Personal Data Protection Bill and the privacy principles established in the landmark Puttaswamy vs Union of India case [16]. Data minimisation, purpose limitation, and explicit consent are integral to the design. To mitigate potential discrimination or exclusion, the system provides fallback options, including OTP-based overrides and optional in-person verification at authorised service centres. This approach ensures that individuals with facial anomalies, limited digital access, or biometric disabilities are not unfairly denied services- a vital consideration due to the digital divide affecting rural and semi-urban regions of India [12].

The system features a compliance dashboard for authorised governmental bodies and telecom regulatory authorities, allowing for regulatory oversight. This dashboard consolidates performance metrics, including verification success rates, opt-out frequencies, and biometric failure cases, while maintaining user anonymity through differential privacy methods. According to Buolamwini and Gebru (2018), these insights are crucial not only for enforcement and policy adjustment but also for ensuring algorithmic fairness and addressing demographic biases in face recognition models [2].

This system can be implemented in stages. First, a pilot program in border states or densely populated areas with significant telecom traffic would gather essential data on user behaviour, failure modes, and technology weaknesses. Following this, a national deployment can commence, utilising telecom operators' current Aadhaar e-KYC integrations and customer outreach channels. Significantly, the system is built for interoperability, facilitating the easy onboarding of new telecom operators, device manufacturers, and government service platforms.

Essentially, the system's framework establishes a dynamic identity ecosystem centred on SIM ownership, where the user's biometric connection is flexible, verified, and preserved over time, location, and device. It provides a strong defence against the misuse of mobile networks in relation to national security threats, integrating intelligence not only in surveillance but also within the core of digital identity assurance. The following sections will place this framework in context across various implementation scenarios, ranging from high-risk border areas to rural regions facing connectivity issues, before examining rollout strategies and fallback options that enhance inclusivity and resilience.

4.2. Scenario-based Implementation Models

The proposed biometric re-authentication system, built on Aadhaar-linked facial recognition, proposes a unified architecture. However, its successful implementation in India's varied sociotechnical landscape demands careful contextualisation. The country's telecommunication infrastructure covers a broad demographic and geographic spectrum, including high-risk border areas, metropolitan centres, remote villages, and underserved rural regions. Each setting poses distinct operational, infrastructural, and behavioural challenges that affect the practicality and effectiveness of biometric SIM verification. Additionally, specific user demographics, such as those with biometric discrepancies or lacking steady access to digital devices, encounter accessibility obstacles that need to be resolved to promote inclusivity and equity in the system's deployment.

This section introduces a tailored implementation model that illustrates how the system can adapt to various user scenarios. It takes into account differences in connectivity, risk sensitivity, user capabilities, and technology acceptance, providing practical recommendations for each situation. These models are crucial not only for deployment logistics but also for fostering user trust, ensuring adherence to privacy regulations, and enhancing system performance in real-world settings. The framework's flexibility across these scenarios highlights its suitability for a phased national rollout, starting with high-risk areas and gradually expanding to larger population segments.

4.2.1. High-risk Users (Border Regions)

Border regions are among the most critical areas for implementing aadhaar-linked biometric sim re-authentication. These locations often represent significant vulnerabilities in national security, facing various illicit cross-border activities, including espionage, arms trafficking, and terrorism. India shares over 15,000 kilometres of land boundaries with seven countries, many of which are geopolitically sensitive. States such as jammu & kashmir, punjab, rajasthan, west bengal, assam, and the northeast encounter ongoing threats from cross-border insurgency and foreign terrorist organisations. According to a report by the indian ministry of home affairs (2021), infiltration attempts and terrorist schemes in these areas commonly involve the use of indian sim cards acquired through fraudulent or proxy means [7]. Consequently, preventing sim misuse in these regions is both a national security necessity and a tactical priority.

In these areas, the adoption of dynamic biometric re-authentication serves as a vital defence tool. By requiring regular facial verification via aadhaar apis, sim card usage becomes directly linked to the individual who originally registered it. Should a verified sim card be passed to another user, especially a foreign agent, it will trigger a flag during the next biometric check, leading to immediate suspension. This approach significantly increases the difficulty of sim-based evasion tactics while ensuring that surveillance and interception technologies rely on trustworthy, identity-verified communication channels.

Telecom operators in border districts can be directed to implement more frequent re-authentication cycles—daily or weekly, depending on risk levels—and utilise geofencing to initiate biometric prompts when a sim crosses established high-risk thresholds. The future availability of 6g's ultra-reliable low-latency communication (urllc) features will

improve the speed and dependability of facial recognition checks even in remote mountainous or forested areas [22]. Until this infrastructure is fully developed, a hybrid approach using 4g/5g along with occasional offline verification at local telecom centres will be required. These centres can have dedicated aadhaar-enabled biometric kiosks as backup solutions in regions with limited mobile bandwidth.

In pakistan's 2015 biometric sim re-verification initiative, a successful model emerged, where more than 100 million sims were verified with fingerprint scanners in sensitive areas. Although this was a one-time operation, it significantly reduced the presence of unregistered sims on the black market and received widespread recognition for enhancing national security [6]. India could benefit from a similar but more advanced and ongoing strategy using facial recognition technology, which offers greater scalability and user convenience, only needing a mobile camera and a secure app, eliminating the need for special hardware or physical presence.

The sensitivity of these areas requires strict logging, oversight, and transparency. Success and failure rates of verifications, instances of opting out, and biometric mismatches should be tracked via real-time dashboards that are accessible to the ministry of home affairs and state law enforcement. The data needs to be anonymised and privacy-respecting, in accordance with the puttaswamy judgement and the forthcoming personal data protection legislation [16, 20]. Despite compliance, the system must remain agile enough to enable prompt cancellation of compromised sims and provide proactive notifications regarding suspicious sim movement patterns, like frequent changes between cell towers near the border.

In summary, high-risk border areas serve as an essential testing ground for the aadhaar-linked re-authentication system. These regions present both heightened risk factors and logistical obstacles that challenge the system's adaptability and resilience. Executing biometric sim verification in these locations not only bolsters india's border security but also serves as a strong deterrent to terrorist use of mobile networks. The lessons learned from these early implementations will shape broader national strategies, enabling a gradual and thoughtful expansion of biometric surveillance that respects both state security and citizen rights.

4.2.2. Low-connectivity Users (Rural Areas)

India's rural and remote areas, crucial for national progress, often provide the toughest settings for implementing digital security systems. The Telecom Regulatory Authority of India (TRAI) reports that approximately 44% of mobile subscribers reside in rural regions. However, these areas frequently fall behind in connectivity quality, smartphone use, and digital literacy [19]. Consequently, any Aadhaar-linked biometric re-authentication system must be carefully designed to operate within existing infrastructural limitations while ensuring inclusiveness and fairness.

In contrast to urban areas or high-risk border regions, rural areas face a critical challenge not in the frequency of SIM misuse for terrorism, but in achieving secure and sustainable identity verification. Many rural inhabitants depend on inexpensive feature phones, often share devices among family members, and experience sporadic electricity and internet availability. As a result, implementing a biometric system that relies solely on regular facial re-authentication via smartphone applications could lead to usability issues. It may exclude a significant segment of the population. According to a 2023 MeitY report, fewer than 30% of rural households have reliable access to high-speed mobile internet, and digital literacy rates are considerably below the national average [12]. Thus, developing solutions for these environments requires not only technical adaptability but also innovative policies.

To overcome these challenges, the biometric re-authentication system should employ a tiered architecture designed for rural settings. In regions with reliable internet and mobile camera access, periodic facial authentication can be conducted through user-friendly app-based interfaces, optimised for low-bandwidth use. The Aadhaar Face Authentication API enables this mode by facilitating facial matching with compressed, encrypted facial vectors instead of high-resolution image streams [20]. In areas with sporadic internet access, the system should permit offline biometric data capture with delayed validation. This process would involve temporarily storing encrypted facial scans on the device and submitting them once the device reconnects to the network, a strategy successfully utilised in rural Aadhaar enrolment camps during the early implementation phase.

In areas where even delayed digital transmission is not possible, fallback solutions are essential. One effective option is to install biometric re-authentication kiosks at local telecom retail shops, community centres, or gram panchayat offices. These kiosks utilise Aadhaar-compatible biometric devices to provide periodic verification points where users can authenticate themselves in person. This type of infrastructure is already proven: India's Common Service Centres (CSCs), encompassing over 600,000 village-level entrepreneurs, have successfully shown that rural access to banking, insurance, and public services is feasible [5].

The system should also support OTP-based verification or SIM-specific security questions as temporary alternatives for users who cannot authenticate biometrically. Nonetheless, these methods must be paired with improved fraud detection algorithms to avert potential misuse. A risk-based authentication framework can be adopted, allowing relaxed re-authentication cycles for low-frequency or low-risk SIM usage, while unusual behaviours, like atypical call destinations or device changes, necessitate biometric prompts or usage limits.

To foster inclusivity in these interventions, telecom operators and regulators should focus on training rural users and raising awareness through campaigns. These initiatives ought to be accessible in local languages, delivered via SMS and IVR, and implemented through outreach programs in part-

nership with non-governmental organisations. The success of India's digital payment initiatives in rural areas, exemplified by programs like DigiGaon and PMGDISHA, which have successfully integrated millions of rural citizens into digital systems, demonstrates that with an appropriate ecosystem and user assistance, even sophisticated biometric technologies can be effectively adopted in remote communities [11].

In summary, rural regions require a flexible, multi-faceted approach to implementing the Aadhaar-linked biometric re-authentication system. While ensuring security against potential SIM misuse is crucial, it's equally important to consider the infrastructural and economic challenges faced by rural India. By incorporating both technological alternatives and community-based support systems, the initiative can guarantee that rural users remain connected without facing undue surveillance compared to the risks involved. This inclusivity not only boosts the system's legitimacy but also affirms that national security measures are genuinely comprehensive across the country.

4.2.3. Users with Disabilities or Biometric Anomalies

One of the most ethically significant challenges in implementing Aadhaar-linked biometric re-authentication is ensuring the fair and smooth participation of individuals with disabilities or biometric anomalies. This user group may be statistically smaller, but it serves as a crucial test of inclusivity within national digital identity systems. The 2011 Census of India indicates that over 2.21% of the population lives with some form of disability, which amounts to more than 26.8 million people [4]. Among these individuals, many may struggle to provide consistent facial recognition data due to issues like facial disfigurement, degenerative muscular disorders, or vision impairments. Additionally, these individuals might also encounter difficulties with fingerprint or iris-based authentication, making them particularly susceptible to exclusion from systems that depend on traditional biometrics.

The Aadhaar framework acknowledges these challenges and offers solutions for handling biometric exceptions, including demographic authentication and manual overrides [20]. However, with the proposed system implementing routine and dynamic re-authentication via facial recognition, it is crucial to enhance these exception mechanisms to maintain access while preventing fraudulent misuse. Upholding fairness and non-discrimination in the system, particularly for differently abled individuals, is not merely a technical requirement but also a constitutional obligation as stipulated by the Rights of Persons with Disabilities Act, 2016 and the wider context of the Puttaswamy privacy ruling [16].

The re-authentication framework should incorporate a layered fallback model. Users identified as having "exception cases" for Aadhaar biometrics may undergo periodic re-verification using demographic-based OTP authentication, custom security questions, or secure in-person verification at specified telecom centres. These centres can feature assistive technologies such as wheelchair-accessible kiosks, screen readers for the visually impaired, and multilingual support interfaces. It is crucial to train telecom staff in accessibility protocols to ensure dignified and effective support for users with disabilities.

Telecom operators and UIDAI must create a grievance redressal mechanism tailored for users facing biometric verification issues. This system should facilitate swift escalation, record challenges, and offer personalised resolution options. Moreover, regular audits and impact evaluations must be carried out to ensure the re-authentication system does not inadvertently exclude individuals with disabilities or those experiencing temporary biometric changes like injuries, surgeries, or the effects of ageing.

Recent progress in AI and deep learning presents promising solutions. Adaptive facial recognition models can be tailored to identify users across various facial conditions and expressions by utilising longitudinal facial data for training. Incorporating multi-modal biometrics, like voice patterns or keystroke dynamics, may provide additional options for users who cannot present typical biometric characteristics. Innovations should adhere to privacy-by-design principles, incorporating user consent, explainability, and data minimisation.

From a policy standpoint, integrating accessibility standards into the Aadhaar-linked SIM authentication guidelines will prevent discrimination in India's digital identity system. The effective implementation of accessible banking services and e-governance initiatives, like the Sugamya Bharat Abhiyan (Accessible India Campaign), shows that scalable and inclusive digital services can be achieved with the support of strategic policies and inclusive design principles [13].

In conclusion, incorporating accessibility into the Aadhaar-linked biometric SIM re-authentication framework is vital for creating a secure and democratic digital environment. By actively responding to the requirements of users with disabilities or biometric differences, the system can achieve its goal of universality, maintaining both technological effectiveness and the ethical obligation of social inclusion.

4.3. Phased Rollout Strategy

Considering India's diverse socio-technical environment, implementing Aadhaar-linked biometric re-authentication for SIM use should occur in a phased and strategically layered approach. Launching it nationwide without prior validation could lead to technical issues, user confusion, infrastructure overload, and pushback from stakeholders not ready for such an operational change. A phased approach, informed by risk awareness, technological preparedness, and demographic inclusivity, promotes ongoing enhancements and supports targeted policy adjustments in real-world settings.

The rollout's initial phase should target high-risk, densely populated urban areas, including border regions, cities with high crime rates, and telecom sectors experiencing significant SIM churn. These areas are critical for national security and

possess a relatively advanced digital infrastructure suitable for pilot testing. Launching in these regions would utilise the existing Aadhaar e-KYC systems of telecom operators, incorporating biometric re-authentication through mobile apps and geo-fenced triggers. According to a 2021 report by the Ministry of Home Affairs, more than 70% of intercepted terrorist communications came from telecom cells near borders [7]. This data positions these areas as optimal for the initial implementation of the system.

At the same time, this pilot phase will provide crucial data regarding system performance, user compliance, failure rates, and technological interoperability. This information can be used to refine backend algorithms and authentication protocols. The findings from the pilot should be openly shared via dashboards accessible to regulatory bodies and civil society organisations, fostering public trust and oversight. This approach is consistent with Cavoukian's (2012) recommendations, highlighting the significance of privacy-by-design and transparency in gaining user acceptance for surveillance technologies [3].

In the second phase, the system should expand into tier-two and tier-three cities, where smartphone usage is growing, yet infrastructural challenges persist. A hybrid approach that combines periodic mobile-based facial authentication with community kiosks for in-person biometric checks should be adopted. This dual-mode strategy ensures that no demographic is left out due to connectivity issues or device limitations. As reported by TRAI (2024), approximately 47% of mobile users in these regions continue to use feature phones or basic smartphones. This factor must be considered when designing user interfaces and authentication prompts [18].

The third phase should concentrate on rural and remote areas, applying insights gained from previous stages while prioritising infrastructure readiness. Initiatives like the Common Service Centres (CSCs) and BharatNet establish a strong foundation for implementing offline or kiosk-based biometric re-authentication [5]. This phase needs significant enhancement through digital literacy campaigns, multilingual training resources, and support systems, ensuring that users grasp both the system's purpose and functionality. Additionally, targeted outreach is essential for tribal communities and economically disadvantaged groups to prevent digital exclusion.

In conjunction with geographic expansion, a rollout sensitive to demographics should be implemented. Users with recognised biometric exceptions, such as individuals with disabilities or those identified during Aadhaar registration as requiring "manual verification," must be onboarded via a distinct channel offering customised fallback options. These users can opt for OTP verification, in-store biometric validation, or delegated verification through certified caregivers or community health officers. The Rights of Persons with Disabilities Act, 2016, requires that no system discriminate based on accessibility challenges, and this principle should be integrated throughout the rollout.

Strict metrics and escalation protocols should guide each phase of implementation. These metrics include authentication success rates, demographic inclusivity indexes, user dropout patterns, and fraud attempt frequencies. A task force, including members from UIDAI, TRAI, the Department of Telecommunications (DoT), and civil society representatives, should review this performance data periodically. Additionally, the phased approach must remain adaptable to legal changes, including the enactment of India's Personal Data Protection Bill and any future amendments to the Aadhaar Act.

In the final phase, the system should evolve into a cohesive national framework that integrates with other digital identity and regulatory systems like CEIR (for device identity), DigiLocker (for secure documentation), and the Aarogya Setu platform (for health user tracking during emergencies). Utilising federated learning models and edge computing made possible by 6G infrastructure, the authentication framework can facilitate ultra-low-latency real-time checks while adhering to strict privacy standards [22].

In conclusion, implementing a phased rollout strategy allows the Aadhaar-linked biometric SIM re-authentication framework to develop naturally within India's telecom and digital identity sectors. This strategy ensures each phase is informed by previous insights, all while upholding transparency, legal standards, and user confidence. Additionally, the phased approach considers the diverse technological, geographical, and socioeconomic aspects of India's population, thus fostering a secure, inclusive, and robust national identity assurance system.

4.4. Fallback Mechanisms

A strong biometric authentication system needs to consider potential technological failures, device constraints, user accessibility challenges, and varying infrastructure. For Aadhaar-linked SIM re-authentication to be effective as a national standard, it should not only rely on robust verification protocols but also incorporate extensive fallback mechanisms that ensure service continuity and inclusivity. Given India's diverse technological environment, characterised by regular power outages, different levels of smartphone access, and inconsistencies in biometrics, a one-size-fits-all method would not address the needs of every user. Consequently, the fallback mechanisms within the proposed system must be practical, scalable, and adhere to both security requirements and individual rights.

The primary and most universally applicable fallback mechanism is OTP-based verification. In cases where users cannot perform facial recognition due to device malfunctions, inadequate lighting, or temporary changes to their appearance from injury or illness, the system should facilitate the generation of one-time passwords sent to either the registered phone number or an alternative verified channel. When this OTP is entered into the telecom provider's portal or mobile

app, it temporarily extends the SIM's active period. However, the use of OTP-based fallback should be limited and implemented with risk-sensitive measures, as it does not have the biometric security of facial recognition and could be vulnerable to social engineering or SIM-swap fraud. Jain et al. (2020) underscore the importance of maintaining a balance between usability and risk mitigation in fallback pathways [8].

Users experiencing ongoing biometric mismatches due to factors like ageing, health conditions, or issues with facial data capture should have access to an in-person re-verification option. This service can be provided at specific biometric kiosks located in local telecom service centres or Common Service Centres (CSCs), which act as rural hubs for e-governance. These kiosks, outfitted with Aadhaar-certified facial and fingerprint scanners, can carry out thorough multi-modal re-authentication and confirm service eligibility. The CSC network includes over 600,000 centres across India, with a significant presence in rural areas, and has proven effective in offering Aadhaar services, banking, and digital education [5].

An important alternative method is to implement scheduled biometric grace periods. Rather than immediately deactivating accounts after a missed re-authentication deadline, the system can initiate a grace phase. During this time, users receive notifications via SMS and are prompted through mobile applications or IVR systems to complete their biometric re-verification. This phase allows for the continuation of essential services, such as incoming calls and access to OTP-based banking, to prevent excessive penalties. This approach is particularly vital for older adults and rural populations who might not respond to digital prompts quickly. TRAI (2024) notes that nearly 46% of mobile users in India continue to depend on basic or mid-tier smartphones, highlighting the necessity of gradual enforcement strategies [18].

Demographic-based verification can also act as a backup, particularly for Aadhaar users who have biometric exceptions. These users can confirm their identity by combining demographic information, such as date of birth, address, or parental details, with behavioural signatures like call patterns or device fingerprints. While this method is not as robust as biometric authentication, pairing it with contextual AI checks can provide a solid security buffer. The Aadhaar Act allows for this alternative verification when biometric authentication is unfeasible [20], which is especially important for users with disabilities or elderly individuals.

As India advances towards 6G infrastructure, fallback systems can leverage ultra-low-latency, context-aware biometric modelling at the edge. Devices with unreliable connections can store biometric attempts and sync them when they reconnect. This enhancement not only increases user flexibility in mountainous or low-signal areas but also alleviates pressure on central servers by distributing verification tasks among edge nodes [22].

A governance layer is essential for overseeing the fallback framework. UIDAI and TRAI must collaborate to establish eligibility guidelines for fallback, set maximum usage limits for OTPs and demographic checks, and ensure the availability of biometric kiosks in underprivileged districts. Regular reviews of anonymised logs for fallback usage are necessary to identify patterns of abuse or systematic barriers to biometric access. Additionally, privacy-preserving methods, such as federated anomaly detection and differential privacy, should be integrated into fallback analytics to safeguard user data while aiding in policy refinement [3].

In conclusion, fallback mechanisms play a crucial role in the proposed biometric re-authentication framework; they enable equity, resilience, and realism. These pathways help ensure that technological failures or user differences do not lead to exclusion or service disruptions. By addressing infrastructural challenges, biometric exceptions, and user diversity, fallback options strengthen the legitimacy, fairness, and national scalability of Aadhaar-linked SIM identity assurance in India.

4.5. Technical Enhancements

The Aadhaar-linked biometric SIM re-authentication system needs a range of technical improvements to guarantee its long-term viability and sustainability. These improvements focus on enhancing system reliability, resilience, and user inclusivity, while also tackling risks like biometric spoofing, environmental variability, and network bottlenecks. Additionally, they ensure the framework adapts to fast-paced technological advancements, especially with the emergence of edge computing, federated AI, and 6G infrastructure.

A crucial improvement is found in AI-driven edge verification. As India advances towards comprehensive 5G implementation and aims for 6G by 2030, there is an increasing potential to shift biometric processing from cloud servers to user devices or telecom edge nodes. AI inference at the edge significantly minimises latency and guarantees that verification processes remain functional even during short connectivity interruptions. Wang et al. (2021) indicate that 6G networks will offer microsecond latency and terabit-speed bandwidth, allowing devices to execute high-speed facial recognition on-site [22]. In rural areas or congested zones, edge processing guarantees reliable authentication experiences, enhancing usability and network scalability.

Geo-fencing and behavioural analytics provide an additional layer of risk-based security. Geo-fencing can initiate facial re-authentication if a SIM card is activated in suspicious or high-risk areas, such as international borders, blocked tower regions, or places notorious for telecom fraud. When combined with behavioural AI models that track anomalies in call duration, contact patterns, or app usage, the system can issue adaptive re-authentication prompts only when unusual activities are detected. This risk-sensitive approach minimises inconvenience for genuine users while improving the identification of SIM misuse without necessitating continuous verification [23].

To prevent presentation attacks, the system needs to implement advanced liveness detection. While basic facial recognition is quick and easy to use, it is vulnerable to spoofing through photos, videos, or deepfake technologies. Adding multi-modal liveness checks—including eye movement tracking, skin reflectance analysis, and passive infrared texture mapping—enhances the robustness of the system. Research by Jain et al. (2020) shows that incorporating multi-sensor input can decrease false acceptance rates in biometric systems by over 90%, making liveness detection a critical enhancement to the authentication process [8].

The proposed framework facilitates continuous learning via federated AI. This method allows mobile devices to locally enhance facial recognition models using users' biometric interactions without sending raw data to central servers. It not only safeguards privacy but also improves algorithm accuracy over time. McMahan et al. (2017) illustrated how federated learning boosts model performance while maintaining user data sovereignty, a concept that is now commonly embraced in healthcare and financial AI sectors [10]. Within the context of SIM authentication, this approach helps ensure that facial verification models stay accurate despite variations related to ageing, lighting, or health conditions.

Another key improvement is the design of context-aware user experiences, especially for digitally marginalised communities. The user interface ought to adjust according to device type, internet quality, and user literacy levels. For example, users with low literacy may get verification prompts using audio in their regional languages, whereas individuals in low-bandwidth regions might access compressed, image-based guides. Additionally, the system should incorporate progressive disclosure, revealing complex explanations only when necessary, to avoid overwhelming or confusing the typical mobile subscriber.

In the data governance layer, features like differential privacy, blockchain audit trails, and zero-knowledge proofs can significantly enhance transparency and data security. For instance, using blockchain logs for each biometric authentication request enables regulators and users to confirm that there has been no unauthorised access or profiling. Additionally, zero-knowledge protocols allow for user identity validation without disclosing biometric details, ensuring compliance with new data protection regulations and the privacy-by-design principles set forth by Cavoukian (2012) [3].

In conclusion, telecom operators need modular API toolkits designed for easy integration of facial re-authentication modules into their current mobile apps, customer portals, and CRM systems. UIDAI should support these APIs by providing documentation, SDKs for both Android and iOS platforms, along with standardised compliance testing protocols. This approach guarantees consistency among operators and speeds up national adoption without the need for developing separate systems from the ground up.

In summary, technical improvements play a crucial role in future-proofing the Aadhaar-linked biometric SIM re-authentication system. They guarantee that the system stays smart, flexible, and secure amid rapid technological changes. By integrating edge computing, behavioural AI, federated learning, and cryptographic privacy solutions, the upgraded system reduces security risks while ensuring that identity assurance keeps pace with India's telecom expansion and its dedication to a digitally inclusive society.

4.6. Regulatory Alignment

The introduction of a biometric re-authentication system linked to Aadhaar for SIM verification should comply with India's current and developing regulatory frameworks concerning digital identity, data protection, and telecommunications. Ensuring this compliance is crucial for legal enforceability, as well as fostering public trust and institutional credibility in a system that fundamentally changes how individual identity relates to accessing mobile communication.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016 establishes the legal framework for Aadhaar-based authentication in both public and private services. According to section 8 of the Act, Aadhaar authentication can be used to verify the identity of individuals accessing services if such authentication is voluntary and based on informed consent [20]. The proposed biometric SIM re-authentication framework can be seen as an extension of this principle. It requires users to periodically verify their identity through facial recognition to maintain uninterrupted mobile service. Notably, while the Aadhaar Act does not specifically require continuous authentication, it does not preclude it, especially when such methods are implemented to address urgent national security concerns and are accompanied by strong protections for user consent and privacy.

Nonetheless, this strategy needs to be aligned with the Supreme Court's pivotal ruling in Justice K.S. Puttaswamy (Retd.) vs Union of India (2017), which defined privacy as a fundamental right per Article 21 of the Indian Constitution [16]. The ruling necessitates a three-pronged assessment of legality, necessity, and proportionality for any policy or system affecting individual privacy. Consequently, the biometric SIM re-authentication system must be substantiated by compelling state interests, such as national security and counter-terrorism, and should utilise the least invasive methods available. Furthermore, the proposal requires robust legal endorsement, preferably through subordinate legislation under the Aadhaar Act or modifications to the Indian Telegraph Rules.

The forthcoming Digital Personal Data Protection Act (DPDP) is a vital parallel framework that establishes guidelines for the lawful collection, processing, and storage of personal data, including biometric information. According to the DPDP Bill, data fiduciaries must obtain explicit and informed consent from individuals for any data processing activities, with the provision for revoking consent at any time.

The biometric re-authentication system must incorporate these principles by providing users with transparency regarding data usage, the option to opt out (with clearly stated service consequences), and opportunities to review and delete stored data whenever possible. Additionally, the principle of data minimisation should be strictly applied, ensuring that only the facial embeddings and metadata necessary for verification are temporarily and securely retained, and that no long-term biometric data is stored at the telecom operator level.

To enhance regulatory oversight, the framework should include auditability features, such as blockchain-based logs of all authentication attempts. These logs can be anonymised for access by regulators like the Telecom Regulatory Authority of India (TRAI), the Department of Telecommunications (DoT), and the proposed Data Protection Board under the DPDP Bill. Since TRAI oversees mobile service providers, it can implement biometric re-authentication requirements within telecom licensing agreements, ensuring they are legally binding through service contracts. Moreover, UIDAI can provide operational guidelines under Section 54 of the Aadhaar Act to standardise re-authentication APIs, fallback protocols, and performance thresholds for service providers.

Global examples reinforce the legality of these actions. Pakistan's biometric SIM re-verification campaign in 2015 was approved under its National Database and Registration Authority (NADRA) laws and has been praised for its legal integrity and effectiveness in enhancing national security [6]. Likewise, in the European Union, GDPR-compliant biometric systems are becoming more prevalent for border security and electronic identity verification, so long as data protection and consent requirements are strictly adhered to.

In India, further alignment with sector-specific regulations may be necessary under the Information Technology Act, 2000, and related rules, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These regulations categorise biometric data as "sensitive personal information" and mandate that it receive enhanced protection. By incorporating these compliance requirements into the proposed system architecture, through measures like encryption, access controls, and regular third-party audits, potential legal disputes can be minimised, and constitutional resilience can be strengthened.

In conclusion, the Aadhaar-linked biometric re-authentication system can operate lawfully and ethically within India's regulatory framework. It aligns with constitutional principles of necessity, proportionality, and informed consent. With suitable safeguards, institutional checks, and transparent implementation methods, this initiative could act as a deterrent against SIM card misuse by terrorist groups while also serving as a benchmark for privacy-focused digital governance in the era of biometric surveillance.

4.7. Cost, Feasibility, and Scalability Considerations

The successful nationwide launch of an Aadhaar-linked biometric SIM re-authentication system necessitates a comprehensive evaluation of cost factors, logistical practicality, and long-term scalability. These considerations are crucial in India, which has more than 1.1 billion mobile connections [18] and where technological adoption varies widely across socio-economic and geographic landscapes. To guarantee that this framework is both financially viable and scalable, it is essential to address financial investments, infrastructure preparedness, technological compatibility, and institutional capacity.

From a cost viewpoint, the primary expenditures involve developing and sustaining telecom-integrated biometric modules, subsidising Aadhaar-based facial authentication services, enhancing access infrastructure in rural locales, and training both staff and users. Currently, Aadhaar authentication services cost ₹0.50 per transaction (UIDAI, 2023), but large-scale deployment across India's mobile user base may lead to significant total costs [21]. Nonetheless, the cost per user is anticipated to decrease with increased scale, particularly since facial recognition utilises existing hardware such as smartphone cameras. Moreover, the marginal expense of implementing software-based authentication through telecom apps is considerably lower than previous biometric approaches like fingerprint or iris scans, which necessitated custom hardware at the service point (Jain et al., 2020).

Feasibility depends on several factors, such as the availability of front-facing camera devices, mobile network access, user digital skills, and the preparedness of telecom companies. As reported by MeitY (2023), over 70% of urban mobile users and approximately 30% of rural users own smartphones that can facilitate biometric authentication [12]. Furthermore, India's expanding 4G and 5G networks improve the feasibility of low-latency biometric verification. With the expected introduction of 6G, these services will achieve even greater efficiency and reliability [22]. Additionally, edge computing and AI-on-device technologies will enable telecom firms to lessen their reliance on cloud services, reducing operational costs while enhancing performance in real-time authentication processes.

From an institutional perspective, the technical and operational viability of this system is bolstered by the availability of existing Aadhaar APIs and the government's prior achievements in large-scale digital initiatives, such as DigiLocker, PMGDISHA, and JAM Trinity. Telecom operators, who currently implement Aadhaar-based e-KYC during activation processes, will need to enhance these systems by adding facial recognition capabilities. Integration toolkits supplied by UIDAI, along with open-source facial recognition frameworks like VGGFace or DeepFace, provide a practical path to deployment without the need to reinvent core infrastructure [14, 17].

Scalability considerations emphasise flexible phased de-

ployment and adaptive architecture. The system is intended to operate in diverse settings, ranging from border security areas that require frequent verification to rural regions where offline data capture and delayed authentication are necessary. As demonstrated in Pakistan's biometric re-verification initiative, scalability can be achieved with appropriate regulatory backing and collaboration between public and private sectors, particularly when it is a national security priority [6]. In India, the CSC ecosystem and the rollout of BharatNet broadband can facilitate the establishment of biometric kiosks and edge-processing nodes in rural locales, forming a basis for inclusive growth [5].

Nonetheless, scalability should not compromise ethical and inclusive design principles. Therefore, it is crucial to implement fallback mechanisms for biometric exceptions, establish secure data governance policies, and create consent-based user interfaces. Leveraging emerging technologies like federated learning and zero-knowledge proofs enables the framework to expand responsibly without centralising sensitive biometric information [3, 10].

To conclude, the Aadhaar-linked biometric SIM re-authentication system is viable and expandable within India's digital environment. While it requires initial investment and necessary infrastructure adjustments, its dependence on established networks, devices, and identity platforms ensures long-term cost-effectiveness. By implementing a phased rollout, providing strong fallback options, and adhering to legal standards, this framework has the potential to serve as a national model for secure digital identity assurance, protecting India's mobile ecosystem while promoting social and economic inclusion.

4.8. Summary

The Solution chapter introduces a thorough, multi-dimensional approach to securing India's mobile network infrastructure via Aadhaar-linked biometric SIM re-authentication. By integrating the system with continuous facial verification linked to the Aadhaar database, this model transitions the SIM card from a static credential to a dynamic and securely connected identity tool. Throughout the chapter, the framework's adaptability to different user scenarios is explored, covering high-risk users in border areas, rural communities with limited connectivity, and individuals with biometric anomalies, thereby ensuring comprehensive coverage while maintaining inclusivity, accessibility, and fairness.

The phased rollout strategy highlights the significance of a gradual, data-informed implementation. It begins with high-priority areas like border zones and urban centres experiencing significant SIM churn, progressively extending to tier-two, rural, and accessibility-sensitive regions. This method allows for real-time policy adjustments and infrastructure alignment. Additionally, fallback mechanisms such as OTP validation, demographic checks, and biometric kiosks provide resilience against technical challenges while protecting user rights. These operational safeguards embody the principle of privacy-by-design and are in accordance with the constitutional protections upheld by the Supreme Court in the Puttaswamy judgment (2017) [16].

This study highlights technological advancements like AI-driven edge processing, federated learning, behavioural biometrics, and liveness detection, showcasing how these future-oriented capabilities can enhance the scalability and reliability of biometric authentication for India's extensive telecom subscriber network. The system aligns with legal frameworks, including the Aadhaar Act, the upcoming Digital Personal Data Protection Bill, and the Information Technology Act, confirming that its implementation is not only technically sound but also legally and ethically justified. Moreover, regulatory collaboration with TRAI and UIDAI, bolstered by blockchain-enabled auditability and user consent measures, strengthens public accountability and fosters institutional trust.

In conclusion, the study explored the essential aspects of cost, feasibility, and scalability. By examining India's successful digital initiatives and utilising the prevalent mobile infrastructure, the framework was demonstrated to be both affordable and logistically achievable. Strategic pilot programs and the integration of existing public service facilities, such as Common Service Centres, provide viable routes for national implementation.

These solutions reflect a vision for secure, inclusive, and ethically sound mobile identity assurance. The next phase of the study will include simulation testing, consultations with stakeholders, and the refinement of performance metrics to guarantee the system is both effective and socially acceptable. Through this initiative, India can establish a globally relevant model for biometric telecom governance, one that prevents misuse, empowers users, and establishes a standard for privacy-centric digital security.

5. Discussion

This study's findings and recommendations illustrate the substantial potential of Aadhaar-linked biometric re-authentication in strengthening India's telecom infrastructure against terrorist misuse and identity fraud. Central to this framework is a transition from static identity verification, prevalent in current SIM registration processes, to a dynamic and ongoing model of biometric validation. This rethinking of identity management in mobile communications is both timely and essential, given the surge in security threats arising from unverified SIM transfers, the digitisation of governance and commerce, and the growing convergence of communication and financial systems.

A key finding from this research is the system's ability to weave security into everyday communication practices. By utilising Aadhaar's established biometric framework and incorporating real-time facial recognition throughout the SIM

lifecycle, identity assurance transforms from being an isolated task at the point of sale to a steady, ongoing process that solidifies the connection between the user and their digital identity. The 2015 biometric SIM verification initiative in Pakistan illustrates this, where over 100 million mobile connections were successfully re-verified [6]. This shows that large-scale biometric implementations are not only possible but can also significantly enhance national security. In contrast, India's technique, which relies on facial recognition instead of fingerprint verification, provides greater scalability and user convenience.

Additionally, the phased and scenario-focused deployment model outlined in this paper emphasises the vital role of context-sensitive implementation. Regions at high risk, such as border states, are supported by frequent re-authentication cycles and geofenced biometric triggers. Conversely, rural and low-connectivity areas need hybrid solutions that merge offline verification methods with mobile-friendly designs and biometric kiosks. Moreover, accommodations for users with disabilities or biometric anomalies reflect a strong dedication to ethical inclusivity and adherence to both constitutional privacy rights and the Rights of Persons with Disabilities Act, 2016. These distinctions highlight the practicality and adaptability of the proposed system across India's diverse demographic landscape.

The system's architecture is designed to be forward-compatible while rooted in current capabilities. It utilises AI-driven edge computing, federated learning, and risk-based behavioural analytics, establishing a foundational groundwork for swift future integration with 6G networks. These components create a privacy-focused infrastructure that enhances verification accuracy, minimises network latency, and safeguards user autonomy. Additionally, the incorporation of zero-knowledge proofs, differential privacy, and federated data training supports a governance model consistent with the Supreme Court's Puttaswamy judgment (2017), ensuring privacy is preserved even as security advances.

However, the system faces several challenges. Implementing it in the real world will necessitate extensive coordination among UIDAI, TRAI, DoT, telecom operators, and local administrative bodies. Although financial aspects are manageable at scale, they still require initial capital and cost-sharing arrangements. Resistance from users may emerge in communities with lower digital literacy or among populations wary of government surveillance. Consequently, the discussion should consider not just operational feasibility but also societal acceptance. Jain et al. (2020) emphasise that maintaining public trust in biometric systems hinges on visible accountability, effective grievance redressal mechanisms, and transparent data practices [8].

The suggested model raises issues regarding its legal enforceability and adaptability to regulations. Although the Aadhaar Act supports Aadhaar-based authentication and will be further strengthened by the upcoming Digital Personal Data Protection Act, the notion of periodic biometric re-authentication is still quite new. Consequently, any extensive implementation will require revisions to the Indian Telegraph Act or its Rules, along with statutory guidelines that specify consent frameworks, data retention policies, and compliance metrics.

In conclusion, the analysis of cost, feasibility, and scalability demonstrates that the solution, though ambitious, is both technically and operationally viable. The existence of over 600,000 CSCs, the expansion of BharatNet broadband, and the rising adoption of Aadhaar-enabled services establish a robust basis for widespread implementation. As the system develops, it has the potential to transform into a versatile identity assurance engine that extends beyond telecommunications to sectors like banking, welfare distribution, e-voting, and more.

In conclusion, this discussion confirms that linking Aadhaar biometric re-authentication to SIM usage serves as a reliable solution for the existing vulnerabilities in mobile network security and simultaneously offers a forward-thinking framework that aligns with India's digital governance goals. Its effectiveness is rooted in its adaptability, inclusivity, and commitment to both constitutional and technological integrity. The next challenge is to convert this vision into a policy-supported, user-accepted, and technically sound national program, one that establishes a global standard for the ethical application of biometric technologies in public security.

6. Conclusion

Considering India's changing national security demands, the Aadhaar-linked biometric re-authentication system for SIM security is both a timely response and a forward-thinking step in digital identity management. This research clearly outlines the key drawbacks of the static identity verification methods currently in use within the country's telecommunication networks. By mapping the transition from Aadhaar-based Know Your Customer (KYC) approaches to a dynamic, real-time identity validation system, the study illustrates how biometric technologies—particularly facial recognition—can act as a vital barrier against the exploitation of SIM cards by terrorist organisations and criminal groups.

The proposed framework reconceptualises SIM ownership as a privilege, dependent on ongoing biometric association rather than a static right. By centring the user in a secure digital ecosystem, the solution guarantees traceable, credible communication channels that are increasingly resistant to impersonation. Combining Aadhaar's national biometric repository with advanced neural networks, this model facilitates inclusive authentication across India's diverse demographics and infrastructure. It accomplishes this via a layered design that addresses high-risk border zones, low-connectivity rural areas, and users with biometric exceptions or disabilities.

Importantly, the solution adheres to India's legal and constitutional principles. Its design principles are rooted in the

Aadhaar Act, the Supreme Court's Puttaswamy ruling, and the envisioned Digital Personal Data Protection legislation. Featuring privacy-by-design, consent-based processes, and federated intelligence, it guarantees the protection of user autonomy and rights, even as national surveillance capabilities are enhanced.

The system is designed to be future-ready. It utilises facial recognition technologies such as DeepFace and VGGFace, accommodates edge computing and federated learning, and is engineered to expand with the upcoming deployment of 6G networks. Its modular design allows telecom operators, policymakers, and technologists to modify and advance the framework without the need for extensive foundational changes. Phased implementation strategies and fallback options ensure resilience against failures and promote fair access across different socio-economic classes.

The Aadhaar-linked re-authentication model is both financially and logistically sound. It leverages current digital infrastructure and demands only minimal investment in software development, training, and user education initiatives. Insights from international examples, including Pakistan's fingerprint-based re-verification efforts, reinforce the practicality of implementing biometric systems nationally for security reasons.

This study enhances the literature on biometric security and digital governance while providing a practical framework to reconcile civil liberties with national safety. It emphasises that, when ethically executed and technologically enhanced, digital identity systems can act as tools for empowerment and shields against subversion. As India modernises its telecom infrastructure, the Aadhaar-linked biometric re-authentication framework becomes critical, aiming to strengthen the country's digital landscape while upholding its democratic principles.

Abbreviations

3D	3-Dimension
4G	4th Generation
5G	5th Generation
6G	6th Generation
AI	Artificial Intelligence
API	Application Programming Interface
CEIR	Central Equipment Identity Register
CNN	Convolutional Neural Network
CRM	Customer Relationship Management
CSC	Common Service Centre
DoT	Department of Telecommunications
DPDP	Digital Personal Data Protection Act
e-KYC	Electronic Know Your Customer
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communication
GSMA	GSM Association
IMEI	International Mobile Equipment Identity
iOS	iPhone Operating System
IVR	Interactive Voice Response
KYC	Know Your Customer
MeitY	Ministry of Electronics and Information Technology
NADRA	National Database and Registration Authority
OTP	One-Time Password
PKI	Public Key Infrastructure
PMGDISHA	Pradhan Mantri Gramin Digital Saksharta Abhiyan
SDK	Software Development Kit
SIM	Subscriber Identity Module
TRAI	Telecom Regulatory Authority of India
UIDAI	Unique Identification Authority of India
URLLC	Ultra-Reliable Low-Latency Communication

Acknowledgments

I am grateful to all my colleagues at Siemens Information Systems Ltd. for equipping me with the knowledge I need to explore the Telecom Domain.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Ball, K., Haggerty, K. D., & Lyon, D. (Eds.). (2012). Routledge handbook of surveillance studies. Routledge.

[2] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of the Conference on Fairness, Accountability and Transparency, 77, 77–91. Retrieved April 22, 2025, from https://proceedings.mlr.press/v81/buolamwini18a.html

[3] Cavoukian, A. (2012). Privacy by Design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. Retrieved April 22, 2025, from https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

[4] Census of India. (2011). Data on disability. Office of the Registrar General & Census Commissioner, India. Retrieved April 22, 2025, from https://censusindia.gov.in

[5] CSC e-Governance. (2023). Common Service Centres: Empowering rural India digitally. Ministry of Electronics and Information Technology, Government of India. Retrieved April 22, 2025, from https://csc.gov.in

[6] GSMA. (2016). Mandatory biometric SIM registration: Lessons from Pakistan. GSMA Intelligence. Retrieved April 22, 2025, from https://www.gsma.com/mobilefordevelopment/resources/mandatory-biometric-sim-registration-lessons-from-pakistan/

[7] Indian Ministry of Home Affairs. (2021). Annual report 2020–2021. Government of India. Retrieved April 22, 2025, from https://www.mha.gov.in

[8] Jain, A. K., Ross, A., & Nandakumar, K. (2020). Introduction to biometrics. Springer. https://doi.org/10.1007/978-1-4614-8219-9

[9] Kaplan, E. H. (2006). Terrorist use of cell phones: A primer on surveillance and countermeasures. Studies in Conflict & Terrorism, 29(3), 307–319. https://doi.org/10.1080/10576100500483431

[10] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), PMLR 54: 1273–1282. Retrieved April 22, 2025, from https://proceedings.mlr.press/v54/mcmahan17a.html

[11] MeitY. (2023). Digital inclusion in rural India: Annual progress report. Ministry of Electronics and Information Technology, Government of India.

[12] MeitY. (2023). India's digital divide and the roadmap for inclusion. Ministry of Electronics and Information Technology, Government of India.

[13] MeitY. (2023). Sugamya Bharat Abhiyan (Accessible India Campaign): Annual report on digital accessibility. Ministry of Electronics and Information Technology, Government of India.

[14] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. British Machine Vision Conference (BMVC). Retrieved April 22, 2025, from https://www.robots.ox.ac.uk/~vgg/publications/2015/Parkhi15/

[15] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 815–823). https://doi.org/10.1109/CVPR.2015.7298682

[16] Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors., Writ Petition (Civil) No. 494 of 2012. Retrieved April 22, 2025, from https://indiankanoon.org/doc/127517806/

[17] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1701–1708). https://doi.org/10.1109/CVPR.2014.220

[18] TRAI. (2024). Telecom subscription data as on December 2023. Telecom Regulatory Authority of India. Retrieved April 22, 2025, from https://www.trai.gov.in/release-publication/reports/telecom-subscription-reports

[19] TRAI. (2024). The Indian telecom services performance indicators: October–December 2023. Telecom Regulatory Authority of India. Retrieved April 22, 2025, from https://www.trai.gov.in/release-publication/reports/performance-indicators-reports

[20] UIDAI. (2017). Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Unique Identification Authority of India. Retrieved April 22, 2025, from https://uidai.gov.in

[21] UIDAI. (2023, May 3). Circular No. 06 of 2023: Pricing of Aadhaar Authentication Transactions. Government of India. Retrieved May 4, 2025, from https://uidai.gov.in/images/resource/Circular_No_06_of_2023_for_pricing_03052023.pdf

[22] Wang, J., Ding, G., Song, J., Yang, Z., & Wang, H. (2021). A survey on 6G wireless communication: Emerging technologies and potential applications. IEEE Communications Surveys & Tutorials, 23(2), 1223–1250. https://doi.org/10.1109/COMST.2021.3058843

[23] Zhou, W., & Piramuthu, S. (2015). Security/privacy of mobile phone apps for health and fitness: A review. Decision Support Systems, 86, 93–101. https://doi.org/10.1016/j.dss.2016.03.005