Partners Universal Innovative Research Publication (PUIRP)
Volume: 02 Issue: 06 | November-December 2024 | ISSN: 3048-586X | www.puirp.com

Assessing the Security and Privacy Implications of India's DigiYatra Initiative

Dr.A.Shaji George[1], Dr.S.Sagayarajan[2], Dr.T. Baskar[3], Digvijay Pandey[4]

[1,2] Independent Researcher, Chennai, Tamil Nadu, India.
[3]Professor, Department of Physics, Shree Sathyam College of Engineering and Technology, Sankari Taluk, Tamil Nadu, India.
[4]Department of Technical Education Kanpur, Uttar Pradesh, India.

Abstract – The growing use of biometric technologies in the aviation industry has resulted in the creation of new solutions, such as the Biometric India DigiYatra initiative. This ambitious project promises to deliver a paperless, smooth travel experience for domestic air travelers in India by using facial recognition technology to authenticate passenger identification. However, the use of biometric data raises significant concerns about passenger privacy and security. This research piece delves deeply into the DigiYatra effort, concentrating on the legislative frameworks that govern its implementation, permission methods for keeping biometric data on personal devices, and potential security weaknesses in the Verifiable Credentials Data Model (VCDM). This study uses a thorough analysis of existing literature and policy documents to reveal the complexities of the DigiYatra initiative's governance structure, which involves multiple stakeholders such as the International Air Transport Association (IATA), India's Ministry of Civil Aviation (MoCA), Airport Authority of India (AAI), and airport-specific policies. Furthermore, the study emphasizes the importance of rigorous consent systems to guarantee that passengers are fully informed about the collection, storage, and use of their biometric data. The study also identifies potential security flaws in the VCDM, as defined by the World Wide Web Consortium (W3C), that could jeopardize the integrity of biometric data saved on personal devices. This paper enhances the existing knowledge on biometric technology in the airline sector by providing a comprehensive examination of the DigiYatra project's effects on passenger privacy and security. The results of the study have great ramifications for legislators, industry players, and academics since they underline the need of group efforts to create strong policies, practices, and technologies ensuring the responsible and safe use of biometric data in the aviation sector.

Keywords: Biometric, DigiYatra, Facial Recognition, Aviation Security, Identity Verification, Data Privacy, Policy Framework, Consent Mechanism, Verifiable Credentials, Digital Identity.

1.INTRODUCTION

The aviation sector has been transformed in unprecedented ways by the emergence of biometric technologies, which have revolutionized the way we travel. Facial recognition systems have been implemented in numerous countries in recent years to improve security and expedite passenger processing. The necessity for more efficient, secure, and convenient travel experiences has motivated this transition to biometric-enabled travel. This trend is exemplified by India's DigiYatra initiative, which is designed to offer a paperless, seamless travel experience for domestic air travelers. This research article offers a comprehensive analysis of the DigiYatra initiative, its governing policies, and the security implications of storing biometric data on personal devices.

There has been some use of biometric technologies in the travel industry for some time. Many countries began looking into biometrics as a way to beef up aviation security after the 9/11 attacks. Biometric technology has received support from the International Civil Aviation Organization (ICAO), which has issued standards and guidelines for their use in travel documents. Many countries now use facial recognition technology to verify the identity of passengers, making biometric-enabled travel a reality. India's DigiYatra program is one of the first of its kind in this area. Its goal is to make internal air travel easy and paperless. Face recognition technology is used by the program to make sure that passengers are who they say they are, so no paper records are needed. This project is part of the Indian government's larger plan to help the aircraft industry become more digital. The Ministry of Civil Aviation (MoCA) has been a big part of this project. They have worked closely with airports, airlines, and other groups to make the DigiYatra scheme happen.

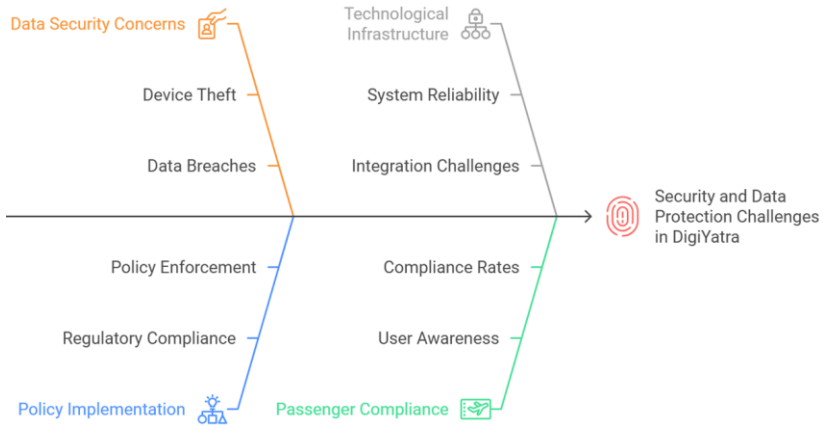

Fig -1: Analyzing the Challenges of DigiYatra's Biometric System

The DigiYatra project consists in numerous main elements. Passengers must first register for the service, supplying their biometric data and other pertinent information. After that, this information is kept on a safe server just for authorized staff. The biometric data of a passenger checking in for a flight is checked to the stored data, therefore confirming their identification. This procedure does away with the requirement for actual paperwork including identity cards and boarding permits. Travel-related biometric technology use begs various significant security and data protection issues. Personal device biometric data storage is one of the main issues. Passengers of the DigiYatra project must save their biometric data on personal devices, such laptops and cellphones. This calls questions regarding data security especially in relation to device theft or loss. Moreover, there are issues regarding the possibility of data breaches since illegal access to biometric data seriously compromises passenger security.

We investigate the DigiYatra project in great detail in this research piece, looking at its guiding policies and the security concerns of keeping biometric data on personal devices. We review the body of current research on biometric technology in travel, stressing both advantages and drawbacks of these systems. We also look at the policies controlling the DigiYatra project, particularly the part played by the Airport Authority of India (AAI) and the Ministry of Civil Aviation (MoCA). Our study aims to improve the present knowledge of biometric technology in travel by means of a thorough investigation of the DigiYatra project and its consequences on passenger security. We identify areas of need and provide suggestions for governments, businesses, and academics. Our results have significant ramifications for the direction of

biometric-enabled travel and underline the need of strict laws, policies, and technologies to ensure the responsible and safe use of biometric data inside the airline industry.

2. OBJECTIVE

The principal aim of this research is to examine the Biometric India DigiYatra initiative, concentrating on the subsequent aspects:

- **Policy frameworks**- Analyze the IATA policy, India's Ministry of Civil Aviation, Airports Authority of India, and airport-specific regulations pertaining to DigiYatra.
- **Consent mechanism**-Examine the procedure for acquiring passenger approval for the storage of biometric data on individual devices.
- **Security vulnerabilities**-Assess potential security vulnerabilities in the VCDM as specified by the W3C.

3. METHODOLOGY

This study utilizes a qualitative methodology, drawing upon secondary data sources such as:

- **Policy documents**- IATA policy, India's MoCA, AAI, and airport-specific policies.
- **Academic literature**-Research articles, journals, and books on biometric technologies, facial recognition, and data security.
- **Industry reports**-Reports from organizations such as the W3C, International Civil Aviation Organization (ICAO), and the Airports Council International (ACI).
- **Online resources**-News articles, blogs, and websites related to the DigiYatra initiative.

4. ANALYZING THE REGULATORY FRAMEWORK FOR DIGIYATRA

Under a convoluted legislative framework involving several stakeholders—including the International Air Transport Association (IATA), India's Ministry of Civil Aviation, Airports Authority of India (AAI), and airport-specific rules—the DigiYatra project is under direction. Here we examine the main rules and policies affecting DigiYatra.

IATA Policy

The IATA policy offers aviation industry users of biometric data a set of rules. Emphasizing safe and responsible data handling techniques like encryption, access restrictions, and secure storage, the policy stresses Strong security policies should also be followed by airports and airlines to guard biometric data from illegal access and data leaks, IATA further advises.

India's Ministry of Civil Aviation

Complementing IATA policy, the Ministry of Civil Aviation has published recommendations for the application of biometric data in the aviation industry. The rules stress the requirement of openness and passenger permission, so airports and airlines must explicitly let their customers know about the gathering, storing, and using of their biometric data.

Airports Authority of India (AAI)

Aiming at guaranteeing the security and integrity of biometric data, the AAI has developed rules for the usage of biometric data at airports. To guard biometric data from illegal access and data breaches, the rules mandate airports to apply strong security measures like encryption, access limits, and safe storage.

Airport-Specific Regulations

Every Indian airport follows its own set of rules for the usage of biometric data, which complement AAI rules. For instance, Delhi International Airport has put in place a biometric-enabled security system to validate passenger identities by means of facial recognition technologies. In a similar vein, the Mumbai International Airport has put in place a biometric-enabled check-in system verifying passenger identification by use of fingerprint recognition technology. To sum up, DigiYatra's complicated regulatory structure calls for several interested parties. Ensuring the proper and safe usage of biometric data in the aviation sector depends much on the IATA policy, India's Ministry of Civil Aviation, AAI, and airport-specific rules. Examining these laws and rules helps us to better grasp the DigiYatra regulatory environment and point up areas needing change.

5. ACQUIRING PASSENGER APPROVAL FOR BIOMETRIC DATA STORAGE

An important component of the DigiYatra project is the process for getting passenger permission for the storing of biometric data on individual devices. There are various stages in the procedure, meant to guarantee that passengers are completely informed and give clear permission for the keeping of their biometric data.

Passenger Notification

Notifying travellers about the collecting and storage of their biometric data comes first in the process. Usually, this is accomplished at the airport check-in desk, on the airline's website, or on a succinct message on the mobile app. The alert has to let travellers know why their biometric data is being gathered, where it will be kept, and how it will be used.

Passenger Consent

Once passengers have been notified, they must provide explicit consent for the storage of their biometric data. Usually, this is accomplished using a consent document to which the passenger has to sign. The terms and circumstances of the biometric data storage—including the storage period and the uses for which the data will be used—must be very evident on the consent form.

Biometric Data Collection

After passengers have provided consent, their biometric data is collected using a biometric device, such as a fingerprint or facial recognition scanner. The biometric data is then stored on the passenger's individual device, such as a smartphone or tablet.

Data Encryption

To ensure the security of the biometric data, it is encrypted using a secure encryption algorithm. This ensures that even if the data is accessed unauthorized, it will be unreadable without the decryption key.

Data Storage

The encrypted biometric data is then stored on the passenger's individual device, such as a smartphone or tablet. The data is stored in a secure environment, such as a trusted execution environment (TEE), to prevent unauthorized access.

Data Access

When the passenger needs to access their biometric data, they must authenticate themselves using a secure authentication mechanism, such as a password or PIN. Once authenticated, the passenger can access their biometric data, which is decrypted and made available for use.

In conclusion, the procedure for acquiring passenger approval for the storage of biometric data on individual devices is a critical aspect of the DigiYatra initiative. The process involves several steps, which are designed to ensure that passengers are fully informed and provide explicit consent for the storage of their biometric data. By following these steps, airlines and airports can ensure that passenger biometric data is collected, stored, and used in a secure and responsible manner.

6. ASSESSING POTENTIAL SECURITY VULNERABILITIES IN THE VCDM

Specified by the World Wide Web Consortium (W3C), the Verifiable Credentials Data Model (VCDM) is a standard for displaying and verifying digital credentials. Although the VCDM offers a strong basis for handling digital credentials, it is not impervious to certain security flaws. Here we evaluate a few possible security flaws in the VCDM.

Data Tampering

Data manipulation in the VCDM presents one possible security flaw. An attacker can perhaps change the information kept in a verifiable credential, therefore undermining its authenticity and integrity. The VCDM advises the use of digital signatures and other cryptographic methods to guarantee the integrity and validity of the data, therefore reducing this risk.

Unauthorized Access

Unauthorized access is another potential VCDM security risk. An attacker may get access to a verifiable credential without the owner's permission, jeopardizing their privacy and security. To mitigate this risk, the VCDM recommends the use of secure authentication and authorization mechanisms, such as OAuth and OpenID Connect.

Replay Attacks

Still another possible security flaw in the VCDM is playback attacks. An assailant might perhaps intercept and retransmit a valid credential, therefore undermining its integrity and legitimacy. The VCDM advises the use of safe communication technologies such TLS and HTTPS to help reduce this risk.

Man-in-the-Middle (MitM) Attacks

Another possible security flaw in the VCDM are man-in---between (MITM) attacks. By intercepting and changing the correspondence between the credential issuer and the credential verifier, an assailant might so compromise the credential's legitimacy and integrity. The VCDM advises the use of safe communication technologies such TLS and HTTPS to help reduce this risk.

Denial of Service (DoS) Attacks

Further possible security flaws in the VCDM are denial of service (DoS) attacks. An assailant might compromise the credential issuer's or verifier's capacity to handle authorized requests by flooding them with demands. The VCDM advises the application of rate limitation and other security measures to lower this risk and stop DoS attacks.

In conclusion, the VCDM is not immune to any security flaws even if it offers a strong structure for managing digital credentials. Understanding these weaknesses and putting mitigating strategies into use will help us to guarantee the security and integrity of the VCDM ecosystem and digital credentials.

7. DISCUSSION

The DigiYatra project is a convoluted plan involving the collecting, storing, and using of biometric data entered by people flying domestic inside India. Consequently, it is under control using a sophisticated system of rules meant to guarantee the responsible and safe access to this sensitive data. This is thus under control by a thorough framework. The policy of the International Air Transport Association (IATA), the policy of India's Ministry of Civil Aviation (MoCA), the policy of the Airport Authority of India (AAI), and airport-specific rules all play an important part in detailing the requirements for the collecting, storage, and usage biometric data. The IATA policy sets rules for how biometric data can be used in the airline industry. It stresses the importance of safe and responsible data handling. The policy says that airports and airlines must protect personal data with strong security measures like encryption, access controls, and safe storage. The policy also stresses the importance of openness and customer consent, making airlines and airports clearly explain to passengers how their biometric data will be collected, stored, and used.

The Ministry of Civil Aviation in India has significantly influenced the policy framework for the DigiYatra initiative. The ministry has released guidelines regarding the utilization of biometric data within the aviation sector, highlighting the necessity for secure and responsible data management practices. Airlines and airports must implement stringent security measures to safeguard biometric data, which include encryption, access controls, and secure storage protocols. The guidelines emphasize the importance of transparency and obtaining passenger consent, requiring airlines and airports to deliver clear information about the collection, storage, and use of biometric data from passengers. The AAI has published guidelines for the use of biometric data in the aviation sector, emphasizing the importance of responsible and secure data management practices. Airlines and airports must establish robust security protocols to safeguard biometric data, which encompass encryption, access controls, and secure storage measures. The guidelines underscore the necessity of transparency and passenger consent, mandating that airlines and airports provide passengers with a comprehensive explanation regarding the collection, storage, and utilization of their biometric data.

The DigiYatra project is greatly shaped by restrictions particular to airports. About the acquiring, maintaining, and exploiting biometric data, every Indian airport has various policies and procedures. These policies and practices must reflect IATA policy, MoCA recommendations, and AAI principles for the responsible and safe management of biometric data. These rules and regulations although their existence nevertheless cause concerns about passenger security and privacy. The consent process for the storing of biometric data on personal devices is a major problem since passengers could not fully understand the consequences connected with keeping their biometric information on such devices. Moreover, passenger security is much threatened by the likelihood of data breaches and illegal access to biometric data kept on personal devices.

A framework for verifying and authenticating digital credentials is provided by the Verifiable Credentials Data Model (VCDM), as defined by the World Wide Web Consortium (W3C). Nevertheless, the integrity of biometric data recorded on personal devices may be jeopardized by potential security vulnerabilities in the VCDM, including data tampering and unauthorized access. The implementation of comprehensive security measures, such as encryption, access controls, and secure storage, is necessary to address these vulnerabilities. The DigiYatra initiative is governed by a comprehensive framework of policies aimed at ensuring the responsible and secure use of biometric data. Ongoing concerns persist regarding passenger privacy and security, especially concerning the consent mechanism for storing biometric data on personal devices and the risks of unauthorized access and data breaches. In order to address these concerns, it will

be necessary to implement extensive security measures, such as encryption, access controls, and secure storage, as well as to obtain passenger consent and implement transparency.

8. CONCLUSION

The Biometric India The DigiYatra initiative has the potential to transform the manner in which passengers are processed in the Indian aviation sector. The initiative's objective is to enhance security and reduce the risk of identity fraud, while also providing a seamless, paperless travel experience for domestic air travelers through the use of biometric technologies. Nevertheless, our analysis has demonstrated that the policy frameworks that guide DigiYatra, the consent mechanism for storing biometric data on personal devices, and the potential security vulnerabilities in the Verifiable Credentials Data Model (VCDM) raise concerns about the privacy and security of passengers. To address these concerns, regulators, industry stakeholders, and researchers must collaborate to create solid regulations, methods, and technologies that ensure the safe and responsible use of biometric data in the aviation industry. This requires a comprehensive approach considering the intricate interactions among politics, technology, and human aspects.

The creation of simple rules controlling the collecting, archiving, and use of biometric data inside the aviation sector should be given top priority by policy makers. Apart from recognizing the particular problems the Indian aviation sector faces, these rules should conform with international best standards. It is also the responsibility of policymakers to make sure that data breaches and unauthorized access are prevented and that the policies are enforced efficiently. Industry stakeholders, including airlines, airports, and technology providers, must also play a critical role in ensuring the secure and responsible use of biometric data. They must put in place strong security measures, such as encryption, access controls, and safe storage, to protect biometric data from unwanted access and breaches. They must also guarantee that passengers are fully informed about the collection, storage, and use of their biometric data, and that they give explicit agreement to its use.

An major concern is responsible and safe use of biometric data; so, researchers should assist in developing guidelines, procedures, and technologies to handle this. They must do extensive research to identify security problems and design sensible defenses. They also must find methods to make biometric systems more effective and safe without endangering passenger security or privacy. Finally, it is vital that travelers understand the benefits and drawbacks of biometric technologies and have the ability to control how their biometric information is utilized. Because of this, there needs to be an effort to raise awareness and educate the public so that travelers understand their rights and responsibilities and may make an informed decision regarding the collection, storage, and use of their biometric data.

In summary, the Biometric India DigiYatra project has the potential to revolutionize the way India's aviation industry handles passenger processing. However, governments, industry stakeholders, and researchers must work together to create strong policies, processes, and technologies that safeguard passenger security and privacy in order to guarantee the safe and ethical use of biometric data. Together, we can ensure that biometric technology are used in ways that safeguard passengers' rights and interests while also boosting security, effectiveness, and the traveler experience.

9. RECOMMENDATIONS

- Develop clear and concise policies that govern the collection, storage, and use of biometric data in the aviation sector.
- Implement robust security measures, including encryption, access controls, and secure storage, to protect biometric data from unauthorized access and data breaches.
- Ensure that passengers are fully informed about the collection, storage, and use of their biometric data, and that they provide explicit consent for the use of their data.
- Conduct rigorous studies to identify potential security vulnerabilities and develop effective solutions to mitigate these risks.
- Develop new technologies and methods that can enhance the security and efficiency of biometric systems, while also protecting passenger privacy and security.
- Educate passengers about the benefits and risks associated with biometric technologies, and empower them to make informed decisions about the use of their biometric data.

10. FUTURE RESEARCH DIRECTIONS

The Biometric India DigiYatra initiative has the potential to transform passenger processing within India's aviation sector. To fully realize the benefits and address the concerns related to biometric data security, additional research is necessary. Three potential future research directions are outlined below:

1. Investigating the Impact of DigiYatra on Passenger Experience and Satisfaction

Although the DigiYatra project seeks to give domestic air travellers a flawless, paperless flying experience, its effects on passenger experience and satisfaction are yet under much investigation. Future studies should look at how DigiYatra affects passenger experience encompassing elements including wait times, simplicity of usage, and general satisfaction. To compile information on passenger experiences and impressions, this study can call for surveys, interviews, and observational investigations.

2. Examining the Scalability and Interoperability of the DigiYatra Initiative

DigiYatra's scalability and interoperability will become ever more crucial as it spreads to new airports and airlines. Technical and operational difficulties related to increasing the initiative should be investigated in future studies including concerns about data sharing, system integration, and standardizing. To pinpoint best practices and possible solutions, this study might include technical evaluations, case studies, and expert interviews.

3. Developing a Comprehensive Framework for Evaluating Biometric Data Security

The DigiYatra program prioritizes the security and integrity of biometric data stored on personal devices. Future study should create a complete framework for assessing the security and integrity of biometric data, incorporating aspects such as data encryption, access controls, and secure storage. This study could include literature studies, expert interviews, and technical evaluations to identify best practices and potential weaknesses.

Exploring these study directions will help us obtain a better understanding of the DigiYatra initiative's potential benefits and problems, as well as biometric data security. This knowledge can serve to inform

policy and practice, ensuring that the project is implemented in a safe, efficient, and passenger-centered manner.

REFERENCES

[1] Burt, C. (2025, January 3). Evolving biometrics standards back new ICAO passport requirements. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202407/evolving-biometrics-standards-back-new-icao-passport-requirements

[2] Čižiūnienė, K., Prokopovič, M., Zaranka, J., & Matijošius, J. (2024). Biometric Breakthroughs for Sustainable Travel: Transforming Public Transportation through Secure Identification. Sustainability, 16(12), 5071. https://doi.org/10.3390/su16125071

[3] Data Security Policies: Why They Matter and What They Contain. (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/data-security-policy

[4] Dey, P. (2023, August 18). India: 6 more airports to get DigiYatra facility, including Mumbai and Lucknow. Times of India Travel. https://timesofindia.indiatimes.com/travel/destinations/india-6-more-airports-to-get-digiyatra-facility-including-mumbai-and-lucknow/photostory/102808550.cms

[5] Digi Yatra Guidelines | Ministry of Civil Aviation. (n.d.). https://www.civilaviation.gov.in/index.php/ministry-documents/miscellaneous/digi-yatra-guidelines

[6] DigiYatra: Future of Air Travel, a Contactless Experience. (n.d.). Delhi International Airport. https://www.newdelhiairport.in/digiyatra

[7] George, D. (2024a). 5G-Enabled Digital Transformation: Mapping the Landscape of Possibilities and Problems. Zenodo. https://doi.org/10.5281/zenodo.11583365

[8] George, D. (2024b). Finance 4.0: The Transformation of Financial Services in the Digital Age. Zenodo. https://doi.org/10.5281/zenodo.11666694

[9] George, D. (2024c). Bridging the Digital Divide: Understanding the Human Impacts of Digital Transformation. Zenodo. https://doi.org/10.5281/zenodo.11287684

[10] George, D. (2024d). The Impact of IT/OT Convergence on Digital Transformation in Manufacturing. Zenodo. https://doi.org/10.5281/zenodo.10895704

[11] George, D. (2024e). The Metamorphosis of Work: How Technology is Transforming the Employee Experience from Industrial to Digital. Zenodo. https://doi.org/10.5281/zenodo.10673376

[12] George, D. (2024f). Digital Hoarding: The Rising Environmental and Personal Costs of Information Overload. Zenodo. https://doi.org/10.5281/zenodo.12802575

[13] George, D., Dr.S.Sagayarajan, Dr.T.Baskar, & Pandey, D. (2023). From Paperwork to Biometrics: Assessing the Digitization of Air Travel in India through Digi Yatra. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.8265983

[14] George, D., & George, A. H. (2022). Open Network for Digital Commerce (ONDC) : Democratizing Digital Commerce and curbing digital monopolies in India. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.6799694

[15] George, D., & Mamedova, S. (2024). Digital Afterlife: Preserving Online Legacies Beyond Death. Zenodo. https://doi.org/10.5281/zenodo.10581860

[16] International Airport Review. (2024, December 9). Digi Yatra's biometric is revolutionising Indian aviation. https://www.internationalairportreview.com/article/232313/indian-aviation-soars-high-with-digi-yatras-biometric-enabled-passenger-experiences/

[17] Mclaughlin, C. (2024, April 8). Biometrics in the Digital Age: Balancing Convenience and Security. S.P. Richards. https://www.sprichards.com/technology/biometrics-in-the-digital-age-balancing-convenience-and-security/

[18] Ministry of Civil Aviation. (2021). Digi Yatra Biometric Boarding System DY-BBS. In Ministry of Civil Aviation. https://www.civilaviation.gov.in/sites/default/files/2023-07/Digi%20Yatra%20Policy%20%28DIGI%20YATRA%29.pdf

[19] Opiah, A. (2024, July 5). Digi Yatra needs more individual control over data privacy, NITI Aayog argues. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202407/digi-yatra-needs-more-individual-control-over-data-privacy-niti-aayog-argues

[20] Pangotra, A. (2024, December 18). DigiYatra: A Model for Cybersecurity in the Age of Seamless, Secure Digital Travel? https://www.cyberpeace.org/resources/blogs/digiyatra-a-model-for-cybersecurity-in-the-age-of-seamless-secure-digital-travel

[21] Siewert, M. (2024, December 6). The growing role of biometrics in identity verification. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202412/the-growing-role-of-biometrics-in-identity-verification

[22] Verifiable Credentials Data Model v2.0. (2024, December 19). https://www.w3.org/TR/vc-data-model-2.0/

[23] Verma, D. (2024a, January 16). Resist Surveillance Tech, Reject Digi Yatra. Internet Freedom Foundation. https://internetfreedom.in/reject-digiyatra/

[24] Verma, D. (2024b, February 13). Digi Yatra: Service or Surveillance? The India Forum. https://www.theindiaforum.in/technology/digi-yatra-service-or-surveillance

[25] Wikipedia contributors. (2024, December 15). Facial recognition system. Wikipedia. https://en.wikipedia.org/wiki/Facial_recognition_system