International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

Building Secure Biometric Systems for Digital Identity Verification in Aviation Mobile Apps

Mahendar Ramidi

Independent Researcher, USA

ABSTRACT: With mobile platforms becoming a part of the aviation business, it is becoming increasingly important to be able to guarantee the security, efficiency, and compliance with privacy requirements of passenger identity verification. The study introduces a new solution to the concept of embedding secure biometric solutions in mobile platforms to verify the digital identity of people during aviation. The offered system utilizes the facial recognition technology, the use of OAuth 2.0-based authentication, permission-based biometric processes, and makes possible contactless passenger confirmation in the mobile check-in and boarding. The paper explains how the system was designed including the protection of privacy, fall back identity as well as the resilience of the system when the number of users using it at once is high. In addition, it deals with session management of secure mobile authentication, which allows adherence to aviation security standards. The findings of the deployment show that the biometric solution can achieve a significant decrease in the check-in time, the better passenger experience, and adherence to the data protection regulations. As the paper illustrates, mobile biometric identity solutions can be a very reliable and more scalable method of enhancing air travel infrastructure, provided with effective privacy controls and security measures, which are in line with the current demands of efficiency and security in digital identity management.

KEYWORDS: Biometric Identity, Aviation Mobile Apps, Facial Recognition, Secure Authentication, OAuth 2.0, Contactless Check-In, Privacy Protection, Mobile Security

I. INTRODUCTION

The intensive development of mobile technology has transformed how passengers interact with the aviation sector, especially in terms of ticketing, check-in and boarding. As the use of smartphones grows, the use of mobile application in improving the overall travel experience is gaining popularity among the airlines. On the one hand, these innovations are associated with multiple advantages, but on the other hand, it also has a serious drawback, which is the security and efficiency of identity verification. With mobile apps emerging as the key interface with the passengers, it is crucial that these platforms should not only be easy to use but have to pass the stringent test of security, privacy, and compliance with the regulations specific to the aviation industry [1] [2].

To address these issues, there is now an opportunity to implement biometric systems to verify the identity of digital identities in aviation mobile application [3]. The biometric systems, based on the use of unique physical or behavioral traits such as fingerprints, facial recognition, or iris scan, are a more secure, more accurate and easier system of verification of identity than other traditional methods of identity verification such as passports or boarding passes [4]. Facial recognition is one of the biometric modalities that have gained prominence as a mobile based identity recognition for identity verification because of its non-invasive nature, accuracy, and it is able to work under diverse environmental conditions, including in a busy airports.

Digital identity verification using biometric systems is changing how the passengers engage with airline services [5]. More specifically, a unified set of these systems in mobile applications of check-in, security, and boarding procedures creates a convenient and contactless experience that is in line with the increasing need of efficiency, safety, and convenience [6]. Nevertheless, in spite of their promise, there are a few challenges to deploying such systems in the aviation applications. They are: resilience of the system at high concurrency, adherence to aviation standards, user privacy and integration of the biometric solution to the overall mobile ecosystem without interfering with current workflows [7].

The proposed research paper endeavors to solve these issues by proposing a secure biometric digital identity system to be used in a large scale commercial airline mobile application. The system suggested in this paper integrates the facial recognition technology with an effective authentication system on the basis of OAuth 2.0, which allows ensuring the security and smooth verification of passengers identity in a contactless environment. The study also discusses the

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

mechanisms of protecting privacy, the fallback mechanisms of identity verification, and the system performance when an increasing number of users use the aviation industry and highlights its potential to improve security and the experience of passengers.

The increasing application of mobile technology in the aviation industry raises the necessity of secure and scalable system that safeguards the information of passengers as well as the airline infrastructure. The growth of mobile users at airports demands a system that is capable of supporting high concurrency and supporting real-time authentication, and is also concurrent with adhering to high aviation standards [8] [9]. Besides, these systems should be equipped with privacy to guarantee safe processing of sensitive personal information, which is consistent with the international data protection standards and the peculiarities of the aviation industry. The biometric authentication systems can solve these issues to offer streamlined process to the passengers and also reduce the risk of identity theft and fraud.

Aviation sector is among the highly sensitive industries in the world with strict measures to provide safety to the passengers, the crew, and the infrastructure. Identity validation forms a very important component of this security structure since it is necessary to verify the identity of the people entering an aircraft so that there are no chances of the unauthorized members of society accessing sensitive spaces. Conventionally, verification of identity in the field of aviation has been based on the use of passport, boarding passes, and even physical documents of identity. Nonetheless, there are quite a number of limitations to these solutions such as the forgery of documents, human error, and inefficiency of the manual checks, particularly when it comes to commercial airports [10].

Implementation of biometric technology in the aviation industry is not new. A variety of biometric-effected systems have already been introduced at most airports in the world in terms of passport control, border security and baggage handling. These systems are efficient in some situations but usually not connected to the overall travel experience of the passenger and take special hardware and infrastructure. Nonetheless, thanks to the availability of smartphones and mobile applications, it is now possible to incorporate biometrics authentication to the passenger experience itself and eliminate the need to install extra equipment and make the process smooth and contact-free [11] [12].

The aim of the study is due to the willingness to develop a holistic system of biometric that can secure identity verification throughout the entire travel experience, including check-in and boarding, using a mobile app that has become a common part of the prototypical passenger. The proposed solution will provide a safe and convenient way to verify biometric identity with the help of facial recognition and OAuth 2.0-based authentication and consent-based workflows, which will not require passengers to carry physical documents or take part in the lengthy manual checks.

The benefits of using biometric authentication to access mobile applications, in addition to its security and convenience, can help to make the entire passenger experience much better. Customers usually experience long queues at registration desks, queues at barriers, and gates into the aircraft, and this may lead to stress, time wastage, and discontent. The streamline process of mobile check-in with use of facial recognition and protected authentication can help minimize wait time, avoid paper boarding passes, and enhance efficiency, at the same time, keeping the security at the highest levels [13].

Although the concept of biometric has gained remarkable development and is being successfully applied to a specific segment of the aviation industry, there is still a disparity in the implementation of biometric identity verification within the larger context of the mobile ecosystem. The biometric systems which are in use are in many cases siloed, meaning that they operate in separate sections of the passenger path, or that they depend on dedicated hardware, which is not necessarily present at all airports. Moreover, the increased adoption of mobile applications to provide services to passengers has introduced new challenges related to security, privacy as well as system performance especially in terms of dealing with large user base in high-concurrency systems like in airports.

Another big issue is the necessity to find a compromise between convenience and security to users. Biometric authentication presents an effective and safe way of checking the identity of passengers, but it has to be introduced in a manner that is both convenient and in accordance to regulatory provisions. Moreover, these systems should also be resilient such that they can process high volumes of passengers in real-time without damaging data privacy and system integrity. The paper aims to discuss these issues by proposing a holistic biometric digital identity system as an extension of the current mobile applications environment, where the system would be secure, private, and efficient throughout the player experience.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

The main goal of the research paper is to develop and deploy a secure biometric system of digital identity authentication in aviation mobile applications. The research has the following scope including:

1. **Facial Recognition Technology Integration**: The paper examines how the facial recognition technology can be integrated into the mobile application to offer a contactless, secure, and efficient identity verification of passengers when checking in and boarding the plane with the mobile phone.
2. **Secure Authentication Framework**: The study introduces a safe mobile authentication system according to the OAuth 2.0, that helps to maintain the security of the session and data and avoids any third parties accessing passenger data.
3. **Privacy and Data Protection**: The paper also talks about privacy protection, such as consent-based workflow and fallback identity verification, to make people manage to meet the data protection regulations, such as the GDPR and similar international standards.
4. **System Resilience and Scalability**: The process measures the system performance when there is high concurrency of users, the research measures the capacity of the system in terms of serving high volumes of passengers without compromising system reliability and responsiveness.
5. **Passenger Experience Optimization**: Lastly, the paper discusses the way the suggested biometric solution enhances the general passenger experience, due to the decrease in the wait time, shorter check-in and boarding procedures, and the necessity to use physical records.

Through these areas of critical concern, this study will prove that biometric systems can be effectively and safely incorporated into mobile apps to increase passenger identity checks in aviation, and thus be part of the future of air travel infrastructure.

II. REVIEW OF RELATED LITERATURE

The adoption of biometric identity checks in the aviation sector is an activity that has been gradually developing through the last several decades. These systems have now become a necessity in the augmentation of security and facilitation of passenger services. Biometric identification, based on distinctive physiological or behavioral traits, provides a more precise and secure system of rather traditional ways of identification, such as passports, boarding passes, and manual identity checks. Aviation is one of the initial users of biometric technologies since it has a high level of security requirements and large numbers of traffic and passengers require to be processed efficiently [5].

Among the most important benefits of biometric systems is the ability to confirm identity in very fast and precise times. The conventional checks on identity are usually physical and time consuming and this may result into delays and lengthy queues and inefficiencies, particularly during the rush time. Biometric systems, however, provide a more simplified method, as it automates the process of identification and eliminates the possibility of human error. It is especially significant in the industry that processes millions of passengers each year where any minor delay can have a widespread impact on the operations [13].

Face recognition is one of the most popular biometric modalities that are used in the aviation sector in recent years. Facial recognition real-time capability enables quick non-invasive identification without physical contact or expensive equipment. Facial recognition systems are being implemented in airports and airlines at different points of the passenger experience, such as check-in, security checkpoint and boarding. Facial recognition is convenient and efficient, which is in line with the increasing demand of contactless services, especially after the global health challenges. One of the advantages is that the passengers are now able to verify their identity by just looking at a camera so that no physical documents and manual verification is required.

Mobile applications are another major change that has occurred in the field of biometric identity verification. Smartphones are now everywhere as the main platform of managing travel. Airlines and airports are integrating the concept of biometric authentication directly into their mobile apps enabling passengers to authenticate their identity directly during the check-in and boarding processes. This does not only make the travelling experience easy but also a convenience as customers can do identity verification activities on their own devices. As mobile applications serve as the main interface of most passenger services, the implementation of biometric systems into them is a natural step that can bring even greater levels of security and user experience.

Biometric verification based on mobile applications should be convenient and user-friendly to make sure that passengers could verify themselves as soon and as effectively as possible. A combination of facial recognition or fingerprint scanning in these applications is a secure way of authenticating the identity of the passenger without the

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

need of any extra hardware or external equipment. The increased use of mobile-based biometric authentication is transforming how airlines and airports manage identity verification, shifting to a more smooth and contactless one [14]. Nonetheless, as much as there are obvious benefits associated with the introduction of biometric systems in the aviation mobile applications, there are obstacles that need to be overcome in order to make them effective and safe. The protection of sensitive personal information is one of the issues. Biometrics data, including face images or prints has a high sensitivity and must be given high data protection. It is very important to be sure that this information is secure because it might result in identity theft or unauthorized access. Since mobile applications are increasingly becoming the core of biometric authentication, both the safety of the biometric data itself and that of the application themselves are increasingly becoming a concern.

The factor of privacy has also been a big issue in the implementation of biometric systems. Misuse, storage, and unauthorized gain of access to the biometric data of passengers might make them reluctant to provide their biometric data. These issues need to be resolved by transparency and high-quality privacy policies that explain the way biometric data are gathered, stored and processed in a clear and straightforward manner. In order to deal with these concerns, consent-based workflows, in which passengers are given the option to either opt-in or opt-out of biometric verification are becoming more popular. This guarantees that the passengers are in control of their data and are able to make informed choices regarding their involvement in the systems of biometrics [15].

The other challenge that should be considered when implementing biometric systems is the issue of scalability and resilience especially in high concurrency environments like airports. An effective biometric identity verification system should be in position to process the large number of passengers in an effective manner particularly during the peak periods. The system needs to be robust against failures as well whereby there should be fallback systems in case the main biometric system is faced with problems. This will be essential in ensuring the seamless operation of the businesses and reduce the inconveniences to the passenger experience.

Since biometric systems are still under development, the tendency to unite these solutions with other high-tech systems, including machine learning and artificial intelligence (AI), is increasing. The accuracy and reliability of biometric systems can be enhanced by means of machine learning algorithms that can learn by using new data and improve their capabilities. It is also possible to use AI and improve the decision-making process, including a way to detect possible fraud or unusual behavior patterns. Biometric technology coupled with machine learning and AI has great potential in enhancing the general security and efficiency in the identity verification exercise by the aviation industry.

To sum up, biometric identity verification systems constitute a part of the current aviation security, evidenced by their efficient, secure and convenient ways of verifying the identity of passengers. Facial recognition and mobile integration have also enhanced the passenger experience as it allows traveling without contacts and check-ins without inconvenience during the travel process. Some of the problems, including data security, privacy issues, and scalability of the system still exist, but thanks to the further development of biometric technologies and mobile platforms application, there is a chance to overcome them. With the aviation industry still adopting biometrics solutions, the future of air travel now appears to be safer, smoother, and more convenient than ever.

III. FRAMEWORK FOR SECURE BIOMETRIC IDENTITY VERIFICATION IN AVIATION MOBILE APPS

Implementation of biometric identity verification in aviation mobile applications will need a holistic structure which will secure, take care of privacy, scalability, and convenience of the users. This part is a proposal of the structure that is to be adopted in the deployment of a secure biometric digital identity system, which will facilitate a hassle-free, efficient and reliable identity check during the passage. The structure dwells upon such features as facial recognition technology, secure authentication systems, privacy protection, system resiliency, and user experience optimization. It is a framework expected to cater to the special security-related issues of the aviation sector and to make sure that the passenger experience is improved and privacy issues are reduced.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

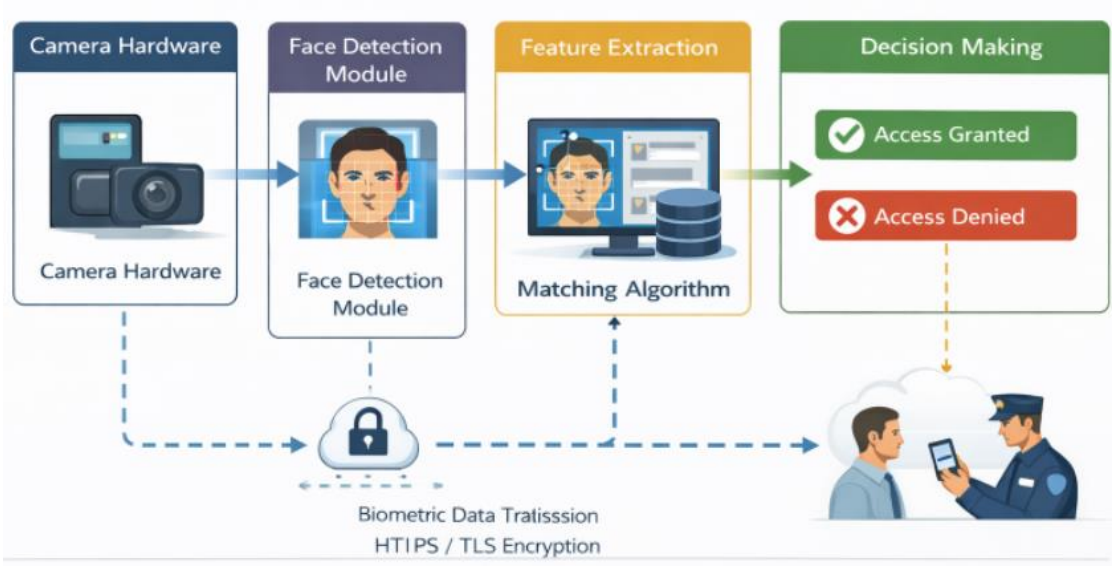

Figure 1: System Architecture for Facial Recognition-Based Biometric Solution

1. Biometric Identification Technology: Facial Recognition Integration

Facial recognition is the heart of the suggested system and will be incorporated into the mobile application that will enable it to verify passenger identity without any difficulties. Facial recognition is preferred because it is non-invasive, it is highly accurate, and it can be used in other environmental settings as well, including airport terminals that are overcrowded. Facial recognition can be made using the built-in camera of the smart phone as compared to the traditional biometric systems which need extra hardware (iris readers or fingerprint scanners). This minimizes the utilization of special infrastructure besides increasing the convenience of the system to passengers.

Facial recognition involves the identification of features that make up the face of the passenger, including the distance between the eyes, nose shape, jawline contour, etc. Such features are further encoded into a digital template which is stored safely in the system. The scan of the face of the passenger is carried out during the verification, and the retrieved image is compared to the stored template. When the match exceeds some threshold, the passenger is admitted and, in such a way, identified correctly and efficiently.

To be able to work in diverse lighting conditions and different distances between the camera and the face of passengers, the system is built to be robust in the real-life conditions. It also uses anti-spoofing strategies, like liveness detection, to avoid fraudulent procedures with the use of photographs or videos.

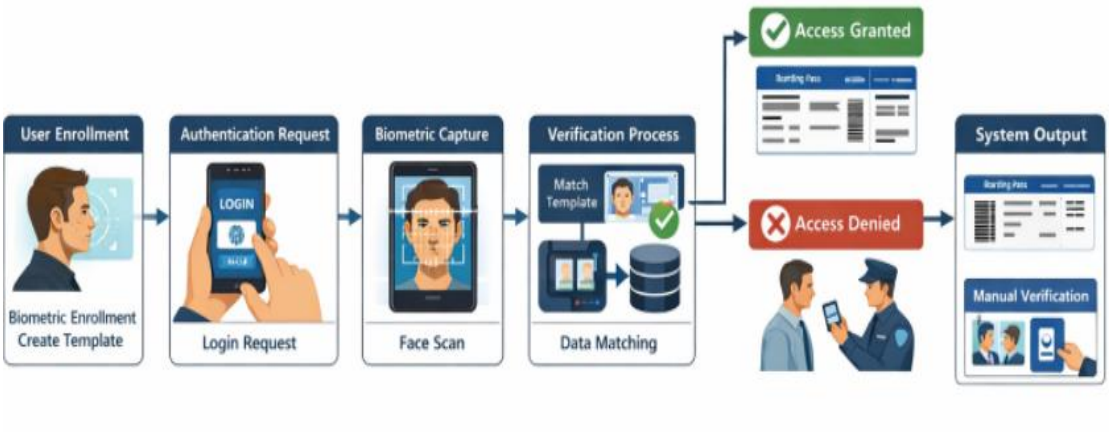

Figure 2: Biometric Authentication Workflow in Aviation Mobile Apps

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

2. Secure Authentication: OAuth 2.0-Based Session Management

In order to stabilize the security of authentication and avoid unauthorized access to sensitive information, the framework has employed the use of OAuth 2.0 based authentication which is a universally accepted industry standard protocol of securing applications access. The OAuth 2.0 enables the system to handle user sessions in a secure way whereby only authorized users can access their digital identity information as well as services.

The process of authentication commences during which the passenger enters the mobile application and the system will initiate a biometric verification (facial recognition). After verifying the identity, the system assigns an authentication token that has a high degree of security and which is representative of the passenger session. This is a token that is used to authorize further actions, like boarding pass retrieval, check-in, and access to other services in the app.

OAuth 2.0 makes transactions between the mobile application and the server securely. The tokens have time restriction and can be canceled in case of a suspicious activity or after the time has elapsed. This enhances an extra level of security as tokens cannot be used in a malicious manner. Moreover, OAuth 2.0 facilitates multi-factor authentication (MFA), which enables the use by passengers of alternative methods of verification, including device-based authentication or two-factor authentication (2FA) to provide the extra security.

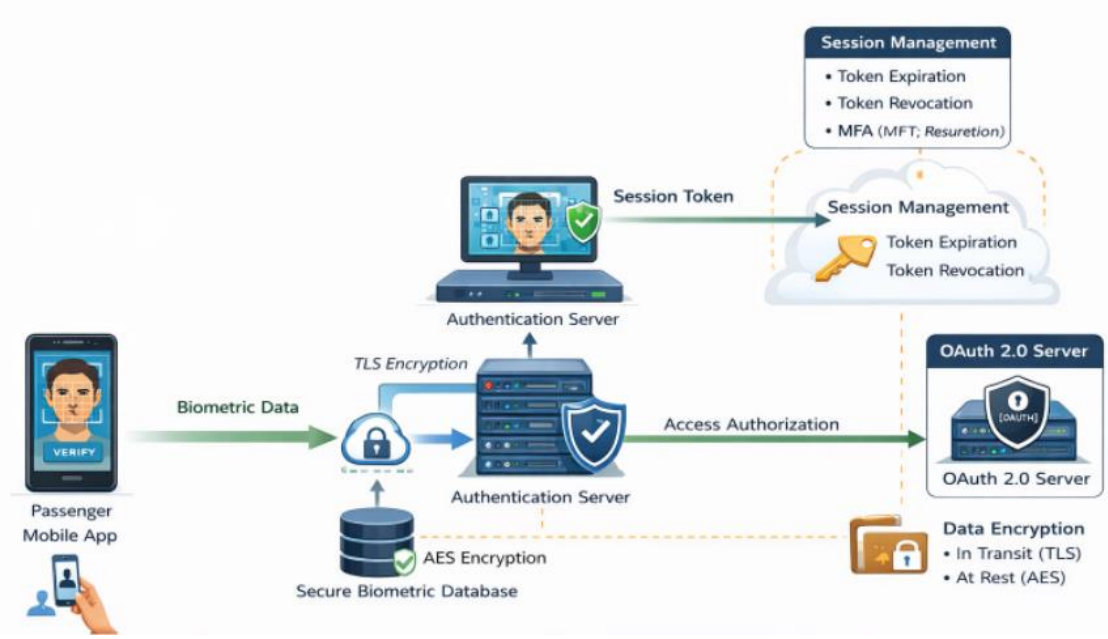

Figure 3: Secure Authentication Architecture with OAuth 2.0 Integration

3. Privacy Protection and Data Security

The biometric information is sensitive by nature, and the procedures of data collection and storage need to be based on the highest privacy and data protection standards. Privacy is one of the main issues in this framework, and a number of mechanisms are introduced to guarantee that the biometric data of the passengers are protected at all points of the process.

3.1 Biometric Workflows through Consent.

The consent-based system of biometric verification is one of the most important characteristics of the system. The passengers are made to explicitly agree to the recording and application of their biometric information towards identity verification before any biometric information is recorded or stored. The system is also equipped with an easy to understand information on the way the data will be utilized, stored, and secured thereby providing the passengers with control over their personal data.

The passengers have the choice to reject biometric verification at any stage with other ways of verifying their identities like regular passport check or manual check by the airport staff. This flexibility guarantees that the passengers are not compelled to provide biometric data, any of which can be used to resolve any privacy concerns.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

3.2 Data Encryption and Secure Storage

Strong encryption is used to ensure the biometric information is secure when transmitting and storing data. The raw images are not kept in the databases but in the form of biometric templates. These templates are hash-encrypted and therefore the reverse engineering of the templates by unauthorized parties is almost impossible and misuse in case of data breach is prevented. The data protection laws of the system are in line with the established data protection laws like the General Data Protection Regulation (GDPR) and other applicable laws, and the biometric data is not stored beyond the required time taken to accomplish the verification process.

Both at rest and transit the data is encrypted, which guarantees the safety of sensitive information over the entire span. Biometric data is protected by means of secure transmission protocols like HTTPS and Transport Layer Security (TLS) as it is transferred between the mobile application, authentication servers, and other system parts. Should there be a breach, this system has provisions of notifying the administrators and automatically locking down the affected accounts to contain the further damages.

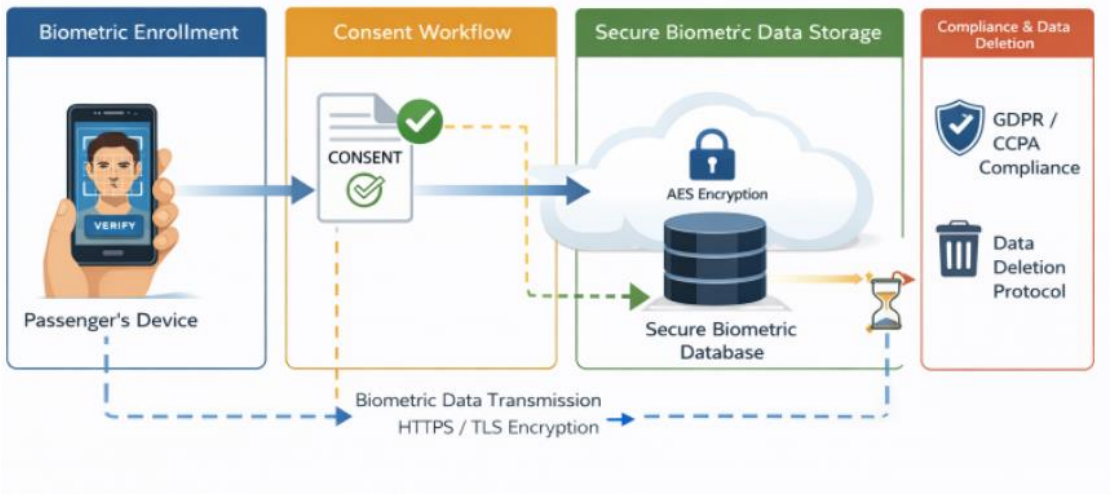

Figure 4: Data Flow for Biometric Information and Privacy Protection

IV. RESILIENCE AND SCALABILITY

Airports are environments involving massive influx of people especially at the peak times and the boldness of the biometric system in terms of scaling and resilience is required. The suggested structure is capable of accommodating large user concurrency without affecting performance, security and reliability.

4.1 High-Concurrency Handling

In order to maintain responsiveness of the system, when the system is heavily loaded, the framework adopts load balancing mechanisms and distributed server architecture. These steps will see that the system is able to handle an extensive number of parallel biometric verification requests without slowing down or failure. Dynamic scaling can be achieved through the utilization of cloud-based infrastructure, which makes the system respond to the changes in the number of passengers very fast.

4.2 Fallback Mechanisms

In spite of the strength of biometric systems, it has situations where the facial recognition might be unable to identify a passenger. The framework also has fallback mechanisms, to be used to make sure the verification process proceeds without problems. When a face recognition does not work, the passengers may be asked to validate it through other means, which may include fingerprint scanning or by relying on the app or an airport system. This will make sure that passengers do not suffer delays or lack of access to the plane because of one point of failure.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

V. USER EXPERIENCE OPTIMIZATION

Security and privacy are a priority though, user experience is also crucial in determining whether the biometric identity verification system is successful. The system is aimed at streamlining the passenger experience by eliminating friction and limiting delays.

5.1 Seamless Integration with Mobile App Ecosystems
The biometric authentication procedure is also perfectly incorporated into the already existing mobile app that is already in place by the passengers. The app will enable the passengers to perform the verification process in a quick and easy manner without requiring to use other hardware or go to different verification counters. This integration makes the journey experience smaller and makes the passengers happier by having a one stop solution to the identity verification and other travelling services.

5.2 Fast and Accurate Authentication
Facial recognition system is also speedy and more accurate such that passengers do not need to spend a lot of time checking their identity. The system will be configured to handle verification requests in real time enabling a hustle free process of check-in and boarding. Also, the system is able to accommodate various diverse passenger situations including the different lighting conditions or even face orientations, and deliver a positive and effective identification.

VI. METHODOLOGY FOR TESTING AND EVALUATING THE SYSTEM

It is important to evaluate the suggested biometric digital identity system in aviation mobile applications to evaluate its effectiveness, performance, security, and user experience. This part describes the approach to testing and evaluation of the system, which will be based on performance metrics, security testing, and deployment outcomes. Evaluation process will involve both the controlled test using laboratory and real world deployment to approximate the real operational condition of a large airport system.

1. Test Environment Setup
A controlled test environment is initially created to examine the biometric identity verification system in an effective way. This is the environment that recreates the conditions of a real-life airport, with changing passenger traffic, light and dark conditions, as well as different user involvement with the mobile application. A test sample is picked to reflect a representative sample, covering the different age groups, gender and ethnicity, so that it can be seen that the facial recognition system will work on the different populations.
The facial recognition technology is implemented in the mobile application, which is launched on various smartphones of various specifications (e.g., iOS and Android phones) to determine its effectiveness in various platforms. The system is linked to a cloud based architecture that models high concurrency to test the scalability and resilience of the system under load.

2. Performance Testing
One of the main elements of the evaluation process is performance testing because the biometric system must be able to process a large number of passenger verification and at the same time be accurate and fast. There are some crucial performance indicators that are established and put to test:

2.1 Authentication Speed
The rate of authentication is another important metric in determining the usability and efficiency of the system. This metric will be used to measure the period between the time a passenger tries authenticating with the help of a facial recognition device until the time they manage to either be authenticated or not. The system needs to offer quick and smooth experience and the average time to authenticate should be less than 2 seconds. Tests are carried out at different conditions such as low-light conditions and crowded conditions to test the flexibility of the system.

2.2 Accuracy and Matching Rate
The accuracy is defined as the capacity of the system to accurately match the passenger biometric with the template on the stored record. The testing measures the False Acceptance Rate (FAR) as well as the False Rejection rate (FRR) of the system, which are the important measurements of accuracy of the system. Low FAR makes sure that the unauthorized persons are not authenticated whereas low FRR makes sure that the legitimate passengers are not rejected. Its optimal value is a FAR of less than 0.1% and FRR of less than 1%. These measures are determined by using a set of real life scenarios in which the system handles biometric data of test subjects.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

2.3 Scalability and Concurrency

Load testing is done to test the capacity of the system to handle high-concurrency conditions, i.e. to simulate a large number of simultaneous authentication requests which is likely to occur during high travel times at an airport. The aim is to determine the ability of the system to hold performance and reliability during times of stress and the response time of the system and the uptime is extremely checked. Load tests are performed with artificial traffic of passengers, and the number of simultaneous requests is gradually increased to estimate the performance of the system at various loads.

2.4 System Resilience

Resilience testing is done to determine the performance of the system under failure or disruption. The testing is done to test the resiliency of the system by mirroring the conditions like network delay, server crashes and temporary gaps. These problems should be recoverable by the system and there should be fallback measures which may include alternative verification to make sure that the passengers are capable of going through the verification procedure even when the biometric system goes wrong.

3. Security Testing

Security testing is of importance because of the sensitivity of biometric information. The security tests carried out are as follows:

3.1 Data Protection and Encryption

Encryption protocols of the system are subjected to test so that the biometric data can be stored and transferred safely. The encryption of all biometric data, such as facial templates, is performed at rest and in transit using standard industry encryption algorithms (e.g. AES-256). Penetration testing is done to determine possible vulnerabilities and weaknesses in the data storing and transmission processes. All risks that may be discovered are resolved using better encrypted methods and secure storage measures.

3.2 Liveness Detection

Liveness detection mechanisms are also challenged in order to avoid spoofing attacks, in which the attacker can even claim to be a legitimate passenger, using photos or videos to trick the security personnel. These mechanisms examine the face features, behavior like eye movement, blinking, and head rotation in that order to guarantee that the person being checked is physically present and not an attempt to cheat the system. The efficacy of liveness detection is established in diverse real-life situations, such as in diverse lighting conditions and angles.

3.3 Privacy Compliance

Data protection regulations, including the GDPR, are reviewed by conducting a set of audits and assessments. System is also tested with the aim that the biometric data are collected, processed and stored as per the legal requirements. Workflow Consent Workflows also undergo testing to ensure that the passengers are made aware of the full utilization and storage of their biometric data. Also, the policies governing data retention within the system are reviewed to make sure that the biometric data is only stored as long as they need to be verified and that they are safely cleared after that.

4. User Experience Evaluation

Another important evaluation criterion is the user experience (UX), and a biometric system should be user-friendly to be implemented on a massive scale. A usability test is conducted with a sample of test participants to determine the ease with which the passengers can use the mobile app and fulfill the verification process. The aspects considered include the following:

4.1 Ease of Use

The participants of the test will be requested to do things like registering with the biometric system, check-in, and board using the mobile application. The surveys and direct feedback are used to gauge their convenience of use and ease with the system. This is aimed at making the system user-friendly and to make the identity verification as uncomplicated as possible to the passengers.

4.2 User Satisfaction

Satisfaction levels among passengers are measured using post-test survey, and issues regarding the system speed, its accuracy and convenience are considered. The participants of the test are asked to evaluate their general satisfaction with the system and the qualitative feedback is gathered to define what needs to be improved. This response is essential in developing the user interface making sure that the system matches the expectations of the passengers.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

4.3 Impact on Wait Times

The effects of the biometric system on total wait times is determined by the duration in which passengers take to go through the verification process with the biometric system and the time it takes passengers to go through the process when using traditional ways (e.g., manual checking of documents). These outcomes will be examined to find out the amount of time the system saves particularly at the peak times, as well as the role it plays in enhancing passenger experience.

5. Deployment Results

The system is then put to test in the real world airport setting after laboratory testing to determine how it works in a real life environment. Monitoring of the results of the deployment is undertaken, with the major metrics being the uptime of the system, passenger throughput, and user feedback. Real-time data is taken to determine the effectiveness of the system in a live system and any problems, which were faced in the course of implementation, are recorded and improve on them.

Benefits and Challenges

There are various advantages that come with the implementation of biometric digital identity verification in the aviation mobile software, but there are also challenges that are encountered which will need to be addressed to have a successful implementation. This section explains the benefits as well as possible challenges of embracing this technology in the airline industry.

Benefits

1.Improved Security and Accuracy: Biometric authentication, especially face recognition, is more secure than when compared to conventional identity verification. It has done away with the chances of frauds due to stolen or forged documents, a more reliable and accurate way of checking the identity of a passenger. Biometric systems are much less prone to impersonation, by utilizing peculiar physiological characteristics.

2.Better Passenger Experience: This is one of the main benefits of biometric verification the passenger experience is improved. The system simplifies the check-in, security screening, and boarding procedures that save much time in waiting and eliminate the use of physical documents. This results in more efficient and quicker airport processes and elevates the level of satisfaction.

3.Non-contact and Effective: The biometric systems offer a touchless method that is especially topical within the framework of universal health issues. The procedure of identity verification will require no face-to-face contact between the passengers, and it will not only minimize the chances of viruses transmission but also contribute to the increased convenience and speed of traveling.

4.Scalability: Since more passengers are being handled in the airports, the biometric identity verification systems can easily scale to high demand times, particularly during peak travel times. These systems are able to handle high volumes of live verifications with cloud-based infrastructure and real-time data processing that does not affect the system performance.

Challenges

1.Privacy Concerns: Biometrics information is very sensitive and its gathering, storage and utilization is a big issue in terms of privacy. Passengers might be reluctant to provide biometric data because they are worried of data violation or abuse. It is important to overcome such concerns by ensuring clear policies of data handling and getting direct permission.

2.System Integration and Compatibility: Mobile applications and integration of biometric systems into the existing airport systems may be complicated. It is important that airlines and airports are compatible among various systems, such as facials recognition software, mobile applications, and back-office databases. This is consuming of resources and time.

3.User Acceptance and Accessibility: Although the biometric systems are supposed to be user-friendly, still some groups of passengers will be reluctant to accept the technology, such as the old people or those with handicaps. It is necessary to make sure that the system is open to everyone traveling with, and offer alternative ways of checking to make it widely adopted.

4.Technical Limitations: Biometric systems especially face recognition can be problematic in certain situations which are poor lighting of the area, a crowd of persons, or when the passengers are wearing face covers. The question of high accuracy in various settings is never an easy task technically and has to be taken care of by continuously optimizing the systems.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

VI. CONCLUSION AND FUTURE WORK

Conclusively, the incorporation of secure biometric identity validation in aviation mobile applications is a big step towards improving the efficiency of passenger identity management and security in aviation mobile applications. With the help of facial recognition and OAuth 2.0-based authentication, the system proposed will provide a contactless, quick, and safe method of verifying the passengers throughout the check-in and boarding processes, as well as, any other travel-related operations. The advantages of better security, increased passenger experience, and scalability of biometric verification make it a good offering to modernize the process of airport operations, as well as to handle the problem of privacy with the help of consent-based workflows and enhanced data protection.

Nonetheless, issues of privacy, complexities in integrating systems, and acceptance among the users should also be handled with keen consideration even though these are disadvantages. These issues together with the technical constraints posed by biometric systems underscore the necessity of constant innovation and improvement so that the system can achieve the security requirements as well as passenger expectations.

To further enhance the proposed system, future work will dwell on some of the areas that will be addressed. To begin with, the study of the accuracy of facial recognition will be important, especially when the conditions are dark or crowded. Addition of complex machine learning algorithms might enhance flexibility in the system and minimize the false rejection rates. Also, the multi-modal biometric (facial recognition with other biometric modalities) could be studied as a way of improving system resilience and inclusivity of the users.

The other path to be developed in the future is the adoption of biometric system with larger airport and airline ecosystems so that it can seamlessly interoperate with other systems. This would enable the passengers to spend biometric verification on a broader spectrum of services, such as baggage claim to access to the lounge, thereby simplifying their traveling experience even more.

Lastly, more research will be conducted to overcome the privacy issues by adopting more sophisticated encryption methods and the adherence to the changing global data protection standards. Further passenger education about the advantages and safety of the biometric verification will also be important in promoting wider use.

REFERENCES

1. Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. International Journal of Information Management Data Insights, 1(1), 2021.
2. Bakker, D. (2015). The Strong Case for Automated Controls at the Border. International Airport Review.
3. Bogicevic, V., Bujisic, M., Bilgihan, A., Yang, W., & Cobanoglu, C. (2017). The Impact of Traveler-Focused Airport Technology on Traveler Satisfaction. Technological Forecasting and Social Change, 123(C), 351-361.
4. Brooks, N. (2016). Reducing the Risks - Airport World Magazine.
5. Burt, C. (2018). San Jose to Become First All-Biometric Airport on U.S. West Coast for International Travel. Biometric Technology Today, 2018(9), p. 12.
6. Caldwell, T. (2015). Market Report: Border Biometrics. Biometric Technology Today, 2015(5), 5-11.
7. CAPA. (2017). Airport Technology – What Passengers Want: Greater Personal Control of the Airport Process. CAPA.
8. Carpenter, D., Maasberg, M., Hicks, C., & Chen, X. (2016). A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system. International Journal of Information Management, 36(5), 735-747.
9. CBP. (2019). Biometrics U.S. Customs and Border Protection. CBP.
10. Cimato, S., Gamassi, M., Piuri, V., Sana, D., Sassi, R., Scotti, F. (2016). Personal Identification and Verification Using Multimodal Biometric Data. IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety.
11. Conghaile, P. (2018). Irish Airports First in Europe with Facial Recognition for US Preclearance. Independent.
12. DHS. (2018). Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide. OIG-18-80.
13. Gamassi, M., Lazzaroni, M., Misino, M., Piuri, V., Sana, D., Scotti, F. (2005). Quality Assessment of Biometric Systems: A Comprehensive Perspective Based on Accuracy and Performance Measurement. IEEE Transactions on Instrumentation and Measurement, 54(4), 1489-1496.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 4, July-August 2022 |

DOI:10.15662/IJEETR.2022.0404005

14. Halpern, N., Mwesiumo, D., Suau-Sanchez, P., Budd, T., Bråthen, S. (2021). The effect of organisational readiness, innovation, airport size and ownership on digital change at airports. Journal of Air Transport Management, 90, Article 101949.
15. Warnock-Smith, D., Graham, A., O'Connell, J.F., & Efthymiou, M. (2021). Impact of COVID-19 on air transport passenger markets: Examining evidence from the Chinese market. Journal of Air Transport Management, 94, Article 102085.