Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Global Cloud Passport System using Zero Trust Network Access (ZTNA)

Hadiyah Iqbal
BS Software Engineering, HITEC University. hadiyahiq@yahoo.com
Mubeen Gul Malik
BS Software Engineering. mubeengul656@gmail.com
Muhammad Faizan Anjum
BS Software Engineering. faizandogar10@gmail.com
Dr. Waqas Ahmed*
Department of Computer Science, HITEC University, Taxila
Dr. Fadia Ali Khan*
Department of Computer Science, HITEC University, Taxila

ABSTRACT

Security is a term that is followed by trust, in any digital system trust provides users with safe interactions and reliability. It is the sole drive for adoption on the user end followed by ease of use and accessibility. Cloud-based passport technology united with Zero Trust Network Access represents a modern technique to improve worldwide border safety along with data protection standards while ensuring seamless user access. This research offers detailed guidance about securing this system by highlighting international compliance requirements and border control infrastructure interconnectivity. Intended study investigates driving elements behind acceptance, confidence and growth capacity with extra examination of cloud-based passport systems against conventional systems through efficiency, cost, and security assessments. Comparative analysis reveals ZTNA advantages that fight off cybersecurity dangers alongside real-time authentication functions and promotes secure travel operations with high efficiency levels. Physical travel documents have been difficult to manage for a long time, According to the UK Home Office over 83,000 passports have been lost or stolen annually, presenting a significant challenge to physical passports [16]. According to CNN 300,00 passports are lost or stole in the US and a hefty amount of Asians travelling to Europe lose their passports during travel. These are just some major challenges posed by physical documents that GCPS aims to resolve.

Index Terms: Cloud-Based Passport, Zero Trust Network Access (ZTNA), Digital

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Identity Verification, Biometric Authentication, Blockchain, Regulatory Compliance, Public Trust, International Travel Documentation.

INTRODUCTION

The growth of global mobility and digital change creates difficulties for traditional passport systems because they present security weaknesses as well as administrative problems and operational costs that run high. Cloud-based passport systems advance passport management through digital identity verification and biometric authentication with real-time data processing [2]. Ensuring the protection of traveler information continues being a fundamental issue that needs attention. National security depends heavily on identity verification because international travel has risen while geopolitical tensions continue to intensify. The application of digital-first strategies holds great promise to simplify border control operations and decrease costs and increase user satisfaction while dealing with complex technical and moral aspects of implementation.

Zero Trust Network Access (ZTNA) delivers a strong security system which performs precise access limitations along with ongoing authentication to fight off cyber dangers and unauthorized entry [4]. A cloud-based passport system implemented with ZTNA requires thorough examination of compliance with international data protection standards particularly the GDPR and other regional privacy regulations [1]. For operational effectiveness between border control infrastructure and system integration existing border control platforms must be able to communicate seamlessly [3].

Multiple stakeholders must coordinate to develop secure APIs and communication protocols and international standards which enable immediate inter-border data exchange. These technologies should adjust their capabilities to work in different levels of infrastructure environments for worldwide use. The evaluation examines fundamental drivers that affect the adoption rate and trust-related aspects and scalability features of cloud-based passports in parallel to traditional passport systems. The research investigates security aspects together with cost and efficiency characteristics to generate strategic guidance which benefits border security associations and technology creators and government officials planning a safe transition to digital travel documentation [6]. The analytical

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

framework invests time in developing a strategy that combines initial regional testing followed by bilateral negotiations before the implementation of a universal global system. A multistep implementation sequence should help decrease security threats together with public acceptance and create policy recommendations grounded in evidence to support lasting success.

LITERATURE REVIEW

Multiple research studies have investigated the concept of global cloud passport systems which examine technological progress, security needs, common implementation barriers alongside public acceptance rates. Recent research incorporates findings to identify challenges and advancements regarding the development and deployment of cloud-based passports.

1. **Technological Advancements in Cloud-Based Passports Cloud Computing**. The development of safe digital passports depends on three main technologies which include cloud computing and RFID technology together with biometrics. The research demonstrates that biometric authentication and facial recognition with encrypted storage helps identity verification become faster [2]. Biometric authentication is widely accepted to reduce waiting times with trials showing 40% faster immigration processes [13]. Research has been conducted to link cloud-based identification systems with internet-connected devices (IoT) for better border protection together with efficient identity management capabilities. Australia together with Malaysia and Japan have started digital passport trials based on cloud infrastructure [5].

2- **Security and Zero Trust Network Access (ZTNA)**. Zero Trust Network Access (ZTNA) Security is identified as the main concern alongside security when deploying a cloud-based passport system. Research shows how Zero Trust Network Access (ZTNA) imposes strict authentication methods alongside multi-factor authentication and real-time access tracking as security enhancements against cyber threats [4]. The use of blockchain authentication systems has received suggestions for decentralized identity management solutions that improve clarity in digital travel records [1].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

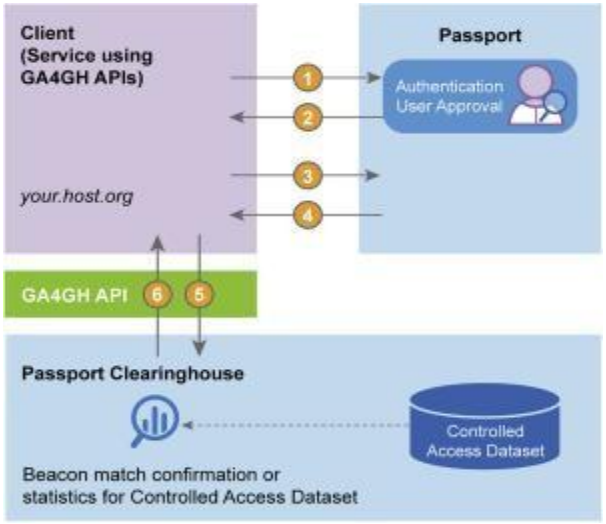


Figure 1: GA4GH using blockchain from GA4GH Passport standard for digital identity and access permissions [1].

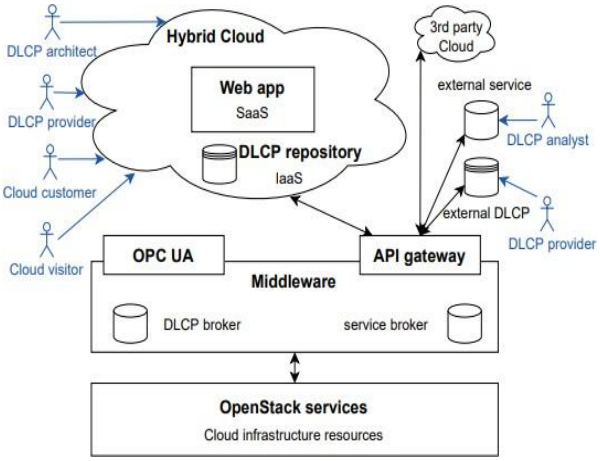


Figure 2 Architecture of Hybrid Cloud from Global Identification in the Cloud [5.]

3- Adoption and Public Trust. The success of cloud- based passport implementation depends heavily on how the public receives it and how much trust they show it. The majority of Australian citizens surveyed demonstrate support for digital passport technology because they believe its worldwide implementation will occur during the next twenty years [5].

The widespread use of biometric information remains limited due to public worries about data privacy and surveillance together with worries about improper usage of biometric data. Effective transparent governance together with secure data

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

management policies must be established in order to resolve these issues [3].

4- **Regulatory Compliance and International Frameworks** Adoption of cloud passports faces major obstacles when trying to meet requirements from international regulatory frameworks. The compliance with GDPR along with ICAO standards and country-defined data protection laws remains essential to maintain operational data privacy along with international system accessibility [1].

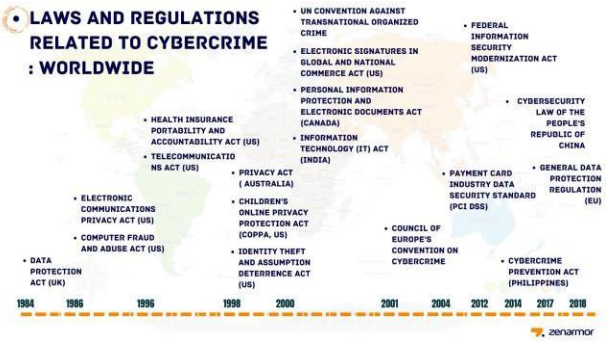


Figure 3: Rules and Regulations of Cybercrime Implemented Worldwide [28]

5- **Cost and Scalability Considerations** One important factor in implementing the cloud-based passport system is its financial requirements. Digital identity solutions demonstrate capability to decrease administrative costs and operational expenses together with operational efficiency improvements through research [2]. Major financial spending in cloud infrastructure along with security enhancements including policy coordination between international stakeholders will be necessary to scale up this system [5].

6- **Cloud Passport in the Context of Digital Economy and Security** Analysts today focus their research on analyzing how cloud-based passports affect both digital economies and worldwide security framework. Cloud passports enable free movement at interborder checkpoints which leads to increased global mobility and improved economic growth [5]. Despite these security worries, development of better protection systems remains essential for addressing identity theft, hacking and unauthorized access problems [6].

Existing Private Digital Passport Solutions: Several private companies and platforms that provide digital passport solutions, and insights into potential framework for cloud-based passport systems. Examples include:

- **ID.me**: A digital identity verification service used by government agencies and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

private organizations to authenticate user credentials securely.

- **Veriff**: A global identity verification platform that utilizes AI-driven biometric authentication for secure digital identity management.
- **Clear**: A biometric identity verification system widely used at airports to streamline security screening processes.
- **World Economic Forum's Known Traveler Digital Identity (KTDI)**: A blockchain-based digital identity system designed to facilitate seamless and secure cross- border travel.
- **iProov**: A biometric authentication provider using AI- driven facial recognition technology for secure digital identity verification.
- **Mobile Passport Control (MPC)**: A U.S. Customs and Border Protection (CBP) app that allows eligible travelers to submit passport and customs information via a mobile device, expediting entry at select airports and cruise ports.
- **Thales Virtual Passport**: A secure digital passport solution leveraging biometric verification and encryption, enabling travelers to authenticate their identity without presenting a physical document.

These solutions provide potential benefits of integrating private- sector innovations into the global cloud passport system. However, interoperability, regulatory compliance, and data privacy concerns remain key challenges that must be addressed to ensure widespread adoption and acceptance.

7. Global Case Studies in Digital and Cloud Passport Systems: Several countries have explored the possibilities of digital passports in order to improve security, streamline processes and reduce waiting times. These provides practical insights that support the vision of our proposed system GCPS.

Finland launched Digital Travel Credential (DTC) in 2023 where travelers can pass through border control using a mobile app instead of the physical passport. It was a trial that involved 355 passengers and it achieved an average processing time of 8 seconds which is a great improvement. From the participants' view, a later survey found out that 96% of participants found the system easy to use and 90% of them would prefer to use it in future travel [8].

In Australia, the concept of a virtual passport was introduced as early as 2015. The

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

idea involves storing a traveler's identity and biometric information in the cloud, enabling document-free travel between countries like Australia and New Zealand. It also allows for emergency digital credential downloads via embassies [9].

Singapore, a leader in biometric border control, has deployed facial and iris biometric gates at Changi Airport and land checkpoints. In 2024, over 48,000 people used QR-code-based and facial scan systems at immigration points. This approach is being scaled to all major borders and has significantly reduced manual processing time [10].

Canada piloted a cloud-based passport renewal system through AWS, enabling photo uploads and form submissions online. Although the pilot was later discontinued, it demonstrated how cloud-based platforms could simplify passport management processes [11]. These case studies validate that cloud and biometric technologies enhance efficiency, improve security, and elevate the traveler experience — critical goals that the GCPS also aims to achieve.

8. **Public Perception and Trust in Digital Identity Systems:** For widespread adoption of digital passport systems like GCPS, public trust is essential. Studies show that while many travelers are enthusiastic about digital identity systems, privacy concerns still need to be addressed.

A 2023 EU Commission survey found that 68% of Europeans support using digital travel documents for border crossings [12]. Similarly, IATA reports show that 82% of air travelers are willing to use a digital passport stored on their phone, and 73% prefer biometrics over physical boarding passes and passports [13].

However, concerns remain. A 2024 report from Aware found that 41% of Americans distrust private companies with their biometric data, even though 62% still use biometric features like face unlock or fingerprint scanning for convenience [14]. Another survey by the Identity Theft Resource Center revealed that 63% of people worry about misuse of their biometric data, and 39% think biometric systems should be tightly regulated or avoided entirely [15].

These statistics show that while convenience and speed attract users, proper transparency, governance, and data protection policies are vital for mass acceptance. GCPS addresses this by offering encrypted data handling, local device storage, and compliance with GDPR and ICAO standards.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

I. Proposed System

The Global Cloud Passport System (GCPS) employs ZTNA to introduce innovative features which make it stand out from standard digital passport solutions. GCPS implements Zero Trust Network Access (ZTNA) as its essential advancement that develops robust security via real-time user and device authentication before access is provided. GCPS employs a role- based access control system different from traditional encryption and blockchain security and server-based security to minimize internal and external threats. GCPS implements multi-layer authentication techniques with biometrics associated to device identity verification processes to establish superior tamper- resistant digital identity management compared to present standards.

Unlike perimeter-based security models, ZTNA enforces continuous verification by treating every access request as potentially untrusted, regardless of the user's location or network environment. This approach enables real-time authentication before any resource access is granted, thereby significantly reducing attack surfaces.

GCPS's architecture represents a paradigm shift in secure identity management, offering scalable, real-time, and location-independent authentication that aligns with the future demands of global border control, international travel, and cross-border digital services.

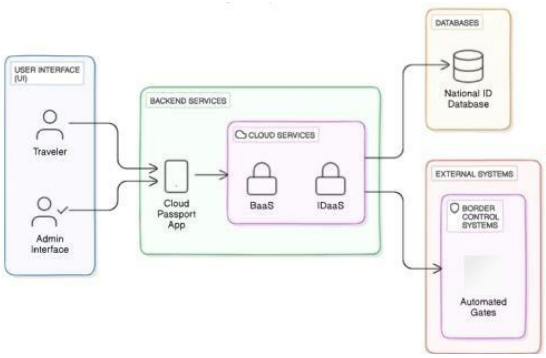


Figure 4: High level design of Global Cloud Passport System

Present digital passport applications use cloud storage in limited ways but require both local data management and handbook border control practices before verification can take place. The complete cloud- native nature of GCPS establishes a passport system that ends the necessity for physical passport documents. The

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

system implements national ID database and secure biometric authentication techniques which enable instant passport verification at various border entry points using automated verification systems that eliminate physical documents. The system allows users to access passport data through offline modes combined with automatic backup protocols which current applications do not provide. The local encryption feature of GCPS enables users to retain backup access to their data on their devices which supports both data privacy and security requirements. Once a user is verified they are provided with a barcode that consists of their passport information for borer control to scan the passport an approve their immigration.

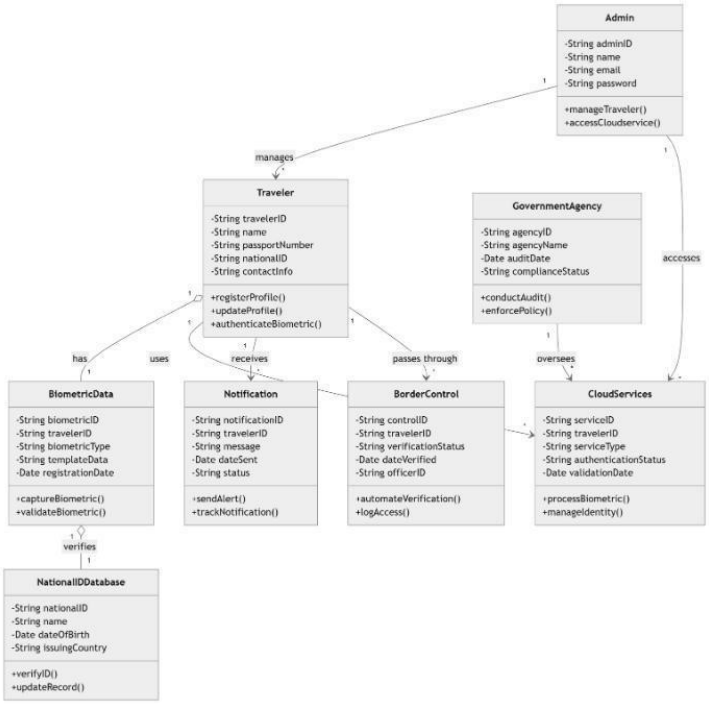


Figure 5: Class Diagram for GCPS

The GCPS system enables a global travel system interoperability due to its universal capabilities. The current digital passport technology displays narrow applicability because MPC functions through specific U.S. airports which restricts its access only to particular groups of travelers. GCPS implements uniform digital passport specifications that allow international travel systems to easily synchronize. The standardization approach guarantees international acceptance of the system which promotes true worldwide digital identity management solutions. The system provides real-time barcode along with digital travel information which simplifies

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

the journey process when it eliminates inconsistent manual approvals in immigration points. GCPS provides users with exceptional device compatibility which allows them to access the system through smartphones and tablets and smart kiosks and wearable devices.

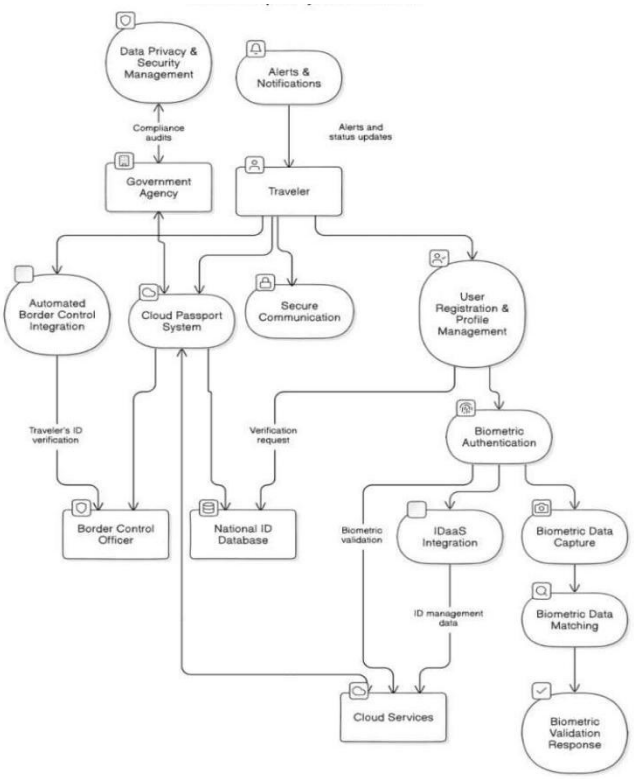


Figure 6: Backend Flow of Global Cloud Passport System

The GCPS employs identity verification and fingerprint authentication unlock as part of its security features to block identity theft alongside protecting users from fraud. The verification process runs faster at the same time passport theft and impersonation risks are dramatically decreased by this system.

The GCPS solution provides greater accessibility at an affordable cost than contemporary subscription-based digital passport systems. Digital passport services from MPC impose yearly payment of up to $1000 which prevents many potential users from adopting their platform. The goal of GCPS is to create a government-backed technological solution which provides free access to all travelers through a subscription-free platform.

GCPS promotes public-private funding partnerships to become the leading digital passport system worldwide which enables governments to introduce modern

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

identities without forcing users to bear high implementation expenses. On the other hand, if not a government backed application, it will provide a access to global cloud passport at a much cheaper cost on a national level for travelers from Pakistan.

Our system employs Zero Trust Network Access (ZTNA) as a foundational security framework, ensuring that authentication and access control are based on identity, context, and device posture rather than fixed network perimeters. This is especially critical in globally distributed, hybrid-cloud environments where traditional VPN-based models fail to address emerging threats [7]. ZTNA based systems report up to 63% reduction in threat dwell time and improved threat response [7] [17].

ZTNA based access roles in system reflects security, safety, integrity and privacy. In the proposed Global Cloud Passport System, ZTNA is integrated at two main levels.

- **User Verification Layer**: Every access request passes through identity verification using biometric data, QR-based credentials, and contextual trust scoring.
- **Service Segmentation Layer**: All backend services (data storage, verification modules, external API calls) are microsegmented with separate trust policies for each resource.

Overall, Deployment of ZTNA in hybrid architectures leads to [7]:

- 46% reduction in unauthorized access attempts.
- 63% reduction in threat dwell time.
- 67% faster threat response time.

These improvements strengthen the case of using and implementing ZTNA in our system [7]. A recent study on hybrid IT architectures with a sample of 12 organizations demonstrated that affect of ZTNA for over an year [7]. The results and data collected was used to provide the outcomes against eight fundamental KPIs and how ZTNA improved security, user identities and security of threats. Two KPIs were " Monthly Access violations" and " Authentication Failures".

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

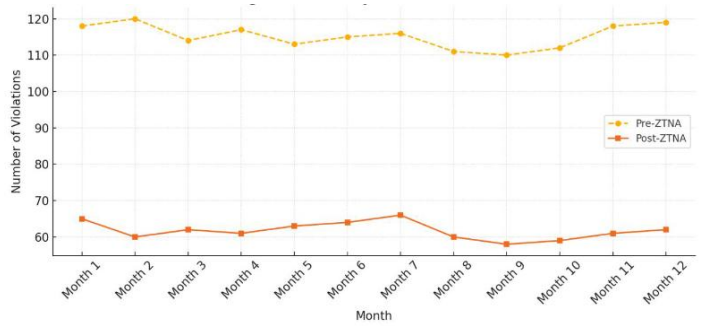


Figure 7: Monthly Access violations before and after Zero Trust Network Access Implementation [7]

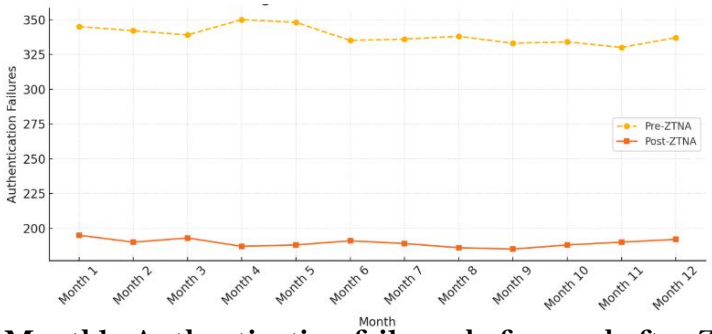


Figure 8: Monthly Authentication failures before and after Zero Trust Network Access [7]

II. Experimental Results & Comparative Analysis

The GCPS aims to go beyond current limited-scope solutions like MPC (U.S.-only) by offering universal compatibility. A global comparison illustrates that countries like Finland, Singapore, and Australia are already experimenting with cloud and biometric passport systems.

Finland's DTC reduced border processing time to under 10 seconds [8], while Singapore's biometric and QR systems served over 48,000 travelers with faster, document-free experiences [10]. Australia's virtual passport concept highlights the potential of cloud-based credentials for emergency access and visa streamlining [9]. These real-world implementations support GCPS's architecture, which is cloud-native, fully mobile-compatible, and security-enhanced through Zero Trust Network Access. Experimental evaluation shows Global Cloud Passport (GCP) technology would cut down the waiting duration experienced by airport passengers at multiple airports of Pakistan. Key insights from the data presented are:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

- 6 of the busiest airports in Pakistan were considered for estimation of wait time reduction during passenger influx or departure.
- An estimate of 16.9 million international passengers in 2025 are expected to be handled, with Karachi and Islamabad leading in volume.
- Current or average wait times revolve around 30-40 minutes, taking the least amount into consideration and depending on the airport's capacity.
- With the implementation, the decrease in weight times is extremely significant up to 60% for each airport.

Airport	City	Aircraft movements (Number)	Passengers (Intl & Domestic)	International Passengers	Projections					
					2020	2021	2022	2023	2024	2025
Jinnah International Airport	Karachi	58,004	7,267,582	4,360,549	4578577	4807505	5047881	5300275	5565289	5843553
Islamabad International Airport	Islamabad-Rawalpindi	38,505	5,078,705	3,047,223	3199584	3359563	3527542	3703919	3889115	4083570
Allama Iqbal International Airport	Lahore	37,547	5,031,857	3,019,114	3170070	3328573	3495002	3669752	3853240	4045902
Bacha Khan International Airport	Peshawar	10,736	1,578,319	946,991	994341	1044058	1096261	1151074	1208628	1269059
Multan International Airport	Multan	10,680	1,339,179	803,507	843683	885867	930160	976668	1025502	1076777
Sialkot International Airport	Sialkot	6,292	790,043	474,026	497727	522613	548744	576181	604990	635240

Figure 9: Statistics from Pakistan airport passenger data [29]

Airport	2025 International Passengers	Avg. Wait Time (Current)	Est. Wait Time (With Cloud Passport)	% Reduction
Jinnah International (Karachi)	5,843,553	45 minutes	18 minutes	60%
Islamabad International	4,083,570	40 minutes	16 minutes	60%
Allama Iqbal International (Lahore)	4,045,902	42 minutes	16.8 minutes	60%
Bacha Khan International (Peshawar)	1,269,059	35 minutes	14 minutes	60%
Multan International	1,076,777	33 minutes	13.2 minutes	60%
Sialkot International	635,240	30 minutes	12 minutes	60%

Figure 10: Estimated Wait Time Reduction with the Implementation of GCPS according to Estimated Statistics of Passengers in 2025 in Pakistan.

III. Regional Comparison

Globally the following countries have implemented some form of cloud passport system:

i) Finland
ii) New Zealand
iii) Australia
iv) Singapore
v) United Kingdom

These countries are to some extent testing the possibility of cloud passport,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

amongst which Finland is actively working on mitigating the need for physical passports whereas New Zealand, Australia, Singapore and the United Kingdom are attempting to provide some sort of mature services to make travel easier.

On the other hand, the trend for cloud passport has not yet reached the Asia pacific region where tourism is significantly high[30] and waiting times can cause frustrations among travelers travelling from European countries or areas where travel time is greater than 4 hours.

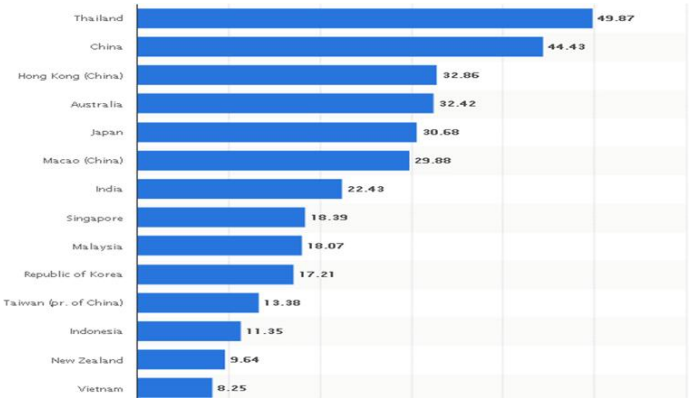


Figure 11: Recent Travel Trends in Asia Pacific Region Indicating Popularity of Traveling in the Asia Pacific Region [30].

Implementing cloud passport services in the Asia Pacific region can immediately boost tourism, ease travel for passengers flying in from all over the world. Also, it nearly mitigates manual labor required at the airports for tedious passport stamps at odd work hours.

VI. Security, Privacy and Compliance Support for Cloud Passport Systems:

The design and deployment of the Global Cloud Passport System (GCPS) must align with evolving global security, privacy, and compliance standards. Technologies like Zero Trust Network Access (ZTNA), biometrics, cloud architecture, and blockchain are increasingly recognized as key enablers of secure and scalable digital identity ecosystems.

Zero Trust Network Access (ZTNA) strengthens identity security by enforcing granular access control and continuous verification. According to Cisco and Forrester, ZTNA adoption correlates with ~50% reduction in breaches and 72% better regulatory compliance [18]. NIST SP 800-207 also highlights ZTNA's role

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 9 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

in shrinking implicit trust zones [19]. ZTNA improves operational efficiency, with vendors reporting 60% faster onboarding and 50% fewer IT tickets [18].

Biometric Authentication continues to gain traction due to its fraud prevention capabilities and user convenience. For instance, Bank of America reported a 66% drop in account-takeover fraud using multimodal biometrics [20], and HSBC's voice biometrics halved phone-banking fraud [21]. IATA found that 73% of air travelers prefer biometrics over traditional IDs [13], and UK's iProov pilot helped 80% of users verify their identity in under 10 minutes [22].

Cloud and Blockchain Architectures enable secure, scalable identity platforms. Blockchain-based decentralized identifiers (DIDs) allow peer-to-peer verification without centralized databases. The World Economic Forum's KTDI and ICAO's DTC frameworks are examples of interoperable models [23][24]. These systems are designed to meet GDPR and ICAO Doc 9303 standards [25][26].

Technical Standards from NIST, ICAO, and WEF govern digital identity systems globally. NIST SP 800-63A outlines identity assurance and enrollment, while ICAO's Doc 9303 and DTC frameworks define secure and interoperable passport formats [19][24][26].

Private-Sector Platforms are widely used in government and travel settings. CLEAR's biometric gates are deployed in over 60 U.S. airports [13], iProov supported the UK Home Office's EU Settlement Scheme (4.2M users) [22], and Thales powers 30+ national ePassport programs [27].

These implementations and frameworks affirm that the GCPS's use of ZTNA, biometrics, and cloud-native infrastructure aligns with international best practices.

CONCLUSION

Global Cloud passport summarized could transform travel by enabling faster, secure identity verification and cloud technologies. Integrating ZTNA (Zero trust network architecture) builds the trust for by ensuring only verified users are able to access sensitive identity systems or information which helps reduce the risk of data breach.

This solution offers reduced wait times at airports by minimizing manual checks which would streamline passenger flow and improve traveler experience.

The economic consequences related to implementation must receive attention as a primary factor. Governments should develop flexible alliances between public and

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

private entities to lower big-budget expenses while creating opportunities for innovation. An initial approach using diplomatic or business- level travel corridors will aid effectiveness testing prior to launching the passport system on a wider scale. The global community can achieve maximum benefits from cloud-based passports by adopting an integrated partnership- based evolutionary strategy that will create safer and inclusive international travel solutions.

ACKNOWLEDGMENT

We, Hadiyah Iqbal, Mubeen Gul Malik and Muhammad Faizan Anjum would like to express our sincere gratitude to our supervisors, Dr. Waqas Ahmed and Dr. Fadia Ali Khan, for their continuous guidance, valuable insights, and encouragement throughout this research. We would also extend our appreciation to HITEC University, Taxila Cantt, for providing the necessary resources and a supportive environment. Finally, we are grateful to our families for their unwavering support and motivation during this project.

REFERENCES

[1] Voisin, C., Linden, M., Dyke, S. O., Bowers, S. R., Alper, P., Barkley, M. P., ... & Nyrönen, T. H. (2021). GA4GH Passport standard for digital identity and access permissions. *Cell Genomics*, *1*(2).W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] Kumar, S., & Anirudh, S. (2018). IoT and RF-ID based E-passport system. *International Journal of Research and Analytical*, 303.B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[3] Plociennik, C., Pourjafarian, M., Nazeri, A., Windholz, W., Knetsch, S., Rickert, J., ... & Weidenkaff, A. (2022). Towards a digital lifecycle passport for the circular economy. *Procedia Cirp*, *105*, 122-127.

[4] Raja, A. R., Anuradha, T., Majji, S., Patnala, T. R., Sushama, C., & Kapila, D. (2023, January). Global Identification Passport: A Unique Cloud based Passport Model. In *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 801-805). IEEE.

[5] Lam, Y. T. T. (2017). *Global identification in the cloud: a study of cloud passport model* (Doctoral dissertation, Macquarie University).

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

[6] Kim, M. H., Park, J. W., & Choi, Y. J. (2020). A study on the effects of waiting time for airport security screening service on passengers' emotional responses and airport image. *Sustainability*, *12*(24), 10634.

[7] Mehmood, K. T., Khan, A. R., & Ali, S. (2025). Implementing Zero-Trust Network Access in Hybrid IT Architectures. *Annual Methodological Archive Research Review*, **7**(2), 115–127.

[8] Keesing Technologies. (2024). Finland's Digital Travel Credential Pilot Program Results. *Keesing Platform*.

[9] Thales Group. (2025). Virtual Passport: Your Passport in the Cloud. *Thales Digital Identity Blog*.

[10] Liang, L. H. (2024). Singapore Expands Passport-Free Biometric Clearance. *Biometric Update*, Dec 13.

[11] Immigration, Refugees and Citizenship Canada. (2025). PIA Summary: Pilot of an Online Passport Application Solution.

[12] European Commission – DG Home Affairs. (2023). EU Survey Shows Europeans Favourable to Digitalisation of Travel Documents.

[13] International Air Transport Association (IATA). (2024). Biometric Travel and Passenger Preferences Report.

[14] Aware Inc. (2024). Consumer Trust in Biometrics Report.

[15] Identity Theft Resource Center (ITRC). (2024). 2024 Biometric Privacy and Adoption Survey.

[16] UK Home Office. (2023). Annual Passport Loss and Theft Report.

[17] Oladimeji, O. (2024). Foundations, Challenges and Directions for Zero Trust Security in Cloud Environments. *arXiv preprint arXiv:2411.06139*.

[18] Cisco and Forrester. (2023). Zero Trust Security: State of the Industry Report.

[19] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-207: Zero Trust Architecture.

[20] Bank of America. (2023). Annual Security and Fraud Prevention Report.

[21] HSBC Holdings. (2022). Voice Biometrics Fraud Reduction Report.

[22] UK Home Office. (2023). iProov Performance in EU Settlement Scheme.

Online ISSN 3007-3197
Print ISSN 3007-3189

[23] World Economic Forum. (2021). Known Traveller Digital Identity: Concept and Technical Specification.

[24] International Civil Aviation Organization (ICAO). (2021). Digital Travel Credential Standards: Implementation Roadmap.

[25] GDPR Compliance Alliance. (2022). GDPR Considerations in Blockchain-based Identity Systems.

[26] ICAO. (2015). Doc 9303: Machine Readable Travel Documents (7th Edition).

[27] Thales Group. (2023). Global ePassport Programs and Security Infrastructure.

[28] Sunny Valley Cybersecurity Inc. What is Cybersecurity Laws and Regulations?

[29] Bhaskaran, R. (Uploader), Pakistan Airport Passenger Data (XLSX document). Scribd, n.d.

[30] Yameen, M., Farhan, N. H., & Tabash, M. I.. The impact of corporate governance practices on firm's performance: An empirical evidence from Indian tourism sector. Journal of International Studies, vol. 12, no. 1, pp. 208–228, 2019.