Article

Not peer-reviewed version

BIPV: Blockchain-Based Identity and Privacy Verification for Airport Passenger Screening Using Circom Groth16 zk-SNARKs

Aaradhya Patangiya and Arokiaraj Jovith A *

Posted Date: 22 April 2026

doi: 10.20944/preprints202604.1543.v1

Keywords: zero-knowledge proofs; Circom; Groth16; zk-SNARKs; blockchain; decentralized identity; airport security; hyperledger fabric; self-sovereign identity; GDPR; privacy-preserving verification; verifiable credentials

 doi:10.20944/preprints202604.1543.v1

Article

BIPV: Blockchain-Based Identity and Privacy Verification for Airport Passenger Screening Using Circom Groth16 zk-SNARKs

Aaradhya Patangiya and Arokiaraj Jovith A *

Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India

* Correspondence: arokiara@srmist.edu.in; Tel.: +91-XXXX-XXXXXX

Abstract

Background: Airport security demands sub-second, high-throughput identity verification while increasingly stringent privacy regulation prohibits the centralized accumulation of passenger data. Existing deployments copy complete passenger profiles to every checkpoint terminal, multiplying the data breach surface at each journey touchpoint and conflicting with GDPR data minimization requirements. **Methods:** This paper presents BIPV (Blockchain-based Identity and Privacy Verification), a system that resolves this tension through programmable zero-knowledge proofs. BIPV anchors only cryptographic references on a Hyperledger Fabric consortium blockchain; passengers prove eligibility at checkpoints via Circom-compiled Groth16 zk-SNARKs that confirm policy compliance without disclosing any underlying personal attributes. We detail the Circom circuit design for airport policy predicates (AgeVerifier, NationalityChecker, DocumentValidator), a proof pre-computation and caching strategy that eliminates gate-lane latency, and a Hyperledger Fabric consortium governance model that anchors verification keys without recording passenger movement. **Results:** Our prototype achieves 0.42 s mean verification latency, 2,380 passengers per checkpoint per hour, and a 94.7% reduction in PII exposure relative to centralized baselines, evaluated across 1,000 simulated verification sessions. Security analysis confirms resistance to credential forgery, replay attacks, and consortium collusion under standard cryptographic assumptions. **Conclusions:** BIPV satisfies GDPR data minimization requirements, ICAO Annex 17, and IATA One ID guidelines. Beyond aviation, the BIPV model generalizes to any domain requiring high-assurance, high-throughput identity verification under privacy obligations.

Keywords: zero-knowledge proofs; Circom; Groth16; zk-SNARKs; blockchain; decentralized identity; airport security; Hyperledger Fabric; self-sovereign identity; GDPR; privacy-preserving verification; verifiable credentials

1. Introduction

Zero-knowledge proofs (ZKPs) have matured from a theoretical cryptographic concept into a practical engineering tool. The Circom toolchain and the Groth16 proving system now allow developers to compile policy predicates—age thresholds, set-membership checks, document validity—into succinct, non-interactive proofs verifiable in milliseconds on commodity hardware [7]. The airport passenger screening domain provides an exacting stress-test for these capabilities: it demands high assurance, sub-second latency, thousands of verifications per hour per checkpoint, and—under the General Data Protection Regulation (GDPR) and IATA One ID—strict minimization of personal data exposure [10,14].

Existing deployments resolve this tension poorly. Centralized systems copy complete passenger profiles (name, passport number, nationality, biometric templates) to every checkpoint terminal, multiplying the breach surface at each of four or more journey touchpoints. A DID-only system that

 doi:10.20944/preprints202604.1543.v1

presents signed credentials reduces exposure somewhat, but verifiers still receive five to seven raw attributes per interaction. BIPV proposes a fundamentally different architecture: passengers carry credentials in a smartphone wallet, generate Circom Groth16 proofs off-line before reaching the security lane, and transmit only Boolean policy outputs to verifiers. Full credential content never leaves the passenger's device at any point.

The system builds on three mature but individually insufficient technologies: Hyperledger Fabric consortium blockchains [4], which allow competing organizations to share a tamper-evident ledger; W3C Decentralized Identifiers (DIDs) and Verifiable Credentials [2,3], which give passengers cryptographic ownership of their identity documents; and Groth16 zk-SNARKs compiled via Circom [7], which let verifiers confirm policy compliance without learning the underlying attributes. Integrating all three into a system that meets the sub-second latency and multi-thousand-passenger-per-hour throughput of a live security checkpoint is the engineering challenge this paper addresses.

This paper makes four principal contributions:

- A Circom circuit library encoding airport policy predicates (age verification, nationality set-membership, document validity) with formal Groth16 soundness guarantees.
- A proof pre-computation and caching strategy that eliminates zk-SNARK proving latency from the live checkpoint interaction, yielding 0.05 s wallet-side contribution to end-to-end latency on a cache hit.
- A Hyperledger Fabric consortium governance model that anchors verification keys and revocation data without recording passenger DIDs or travel history on-chain.
- A prototype evaluation across 1,000 simulated verification sessions demonstrating 2,380 passengers per checkpoint per hour, 0.42 s mean latency, and a 94.7% reduction in PII exposure relative to a centralized baseline.

The rest of this paper is organized as follows. Section 2 reviews background and related work. Section 3 defines the system entities and threat model. Section 4 presents the Circom zk-SNARK design and BIPV architecture. Section 5 provides implementation and evaluation results. Section 6 presents the security and compliance analysis. Section 7 discusses limitations, deployment considerations, and generalization. Section 8 concludes.

2. Background and Related Work

2.1. Zero-Knowledge Proofs and the Circom Toolchain

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) allow a prover to convince a verifier that a computation was performed correctly, revealing nothing beyond the result [7]. The Groth16 proving system produces proofs of a few hundred bytes regardless of circuit complexity and verifies in well under 50 ms on commodity hardware. Circom is a domain-specific language that compiles predicate descriptions into arithmetic circuits compatible with Groth16. The snarkjs library performs proof generation and verification in JavaScript, making it compatible with both browser and React Native environments. Prior work has deployed Circom in anonymous credential issuance [8] and privacy-preserving UAV flight path verification [11]; BIPV extends this to high-throughput physical access control.

2.2. Decentralized Identity and Self-Sovereign Identity

The W3C Decentralized Identifiers (DIDs) specification [2] provides globally resolvable, subject-controlled identifiers that require no central registrar. Paired with Verifiable Credentials (VCs) [3]—cryptographically signed assertions stored in a user wallet—DIDs enable offline or semi-offline identity verification without querying the issuer's database. Self-sovereign identity (SSI) [1] holds that users should control what attributes they share and with whom. Combined with ZKPs, SSI can achieve full zero-disclosure verification—the user proves a predicate holds without revealing the

 doi:10.20944/preprints202604.1543.v1

underlying credential attributes. GDPR's data minimization and privacy-by-design requirements are naturally satisfied by this model [10].

2.3. Hyperledger Fabric for Multi-Stakeholder Consortia

Hyperledger Fabric is a permissioned enterprise blockchain framework in which every participant authenticates via X.509 certificates issued by a Membership Service Provider (MSP) [4]. Channel-based data partitioning lets organizations share only relevant ledger segments, and Go or Node.js chaincode enforces access control policies. These properties make Fabric well-suited to settings where competing organizations—airlines, airport operators, border agencies—must share infrastructure without ceding unilateral control. Chen et al. [6] used Fabric for cross-border digital vaccine credentials; their system, however, does not employ zk-SNARK selective disclosure and was not designed for sub-second, high-volume checkpoint verification.

2.4. Privacy Challenges in Airport Identity Systems

Studies of biometric deployments at airports consistently find that data collected far exceeds what security decisions require [13]. GDPR's purpose limitation and data subject rights conflict directly with the long-term, multi-party repositories that most airports maintain. IATA One ID [14] articulates a vision of pre-validated digital identity reused across journey touchpoints, but leaves open how that information should be protected in transit and at rest. BIPV provides a concrete technical foundation for the One ID vision—one that uses cryptographic proofs rather than data-sharing agreements to achieve interoperability.

3. System and Threat Model

3.1. System Entities

BIPV involves five principal classes. The **Passenger** holds one or more validated credentials in a smartphone wallet and generates zero-knowledge proofs in response to checkpoint requests. The **Issuer**—a government ministry, airline, or accredited identity provider—creates and cryptographically signs credentials tied to the passenger's DID. The **Verifier** operates a checkpoint terminal at a security lane, check-in desk, or border station and uses proof bundles to render access decisions. The **Consortium Network** is a Hyperledger Fabric instance jointly administered by all participating organizations, serving as the authoritative registry for issuer DIDs, credential schemas, verification keys, and revocation data. The **Governance Committee** is the consortium body responsible for admission policies, schema approval, key management procedures, and regulatory compliance oversight.

3.2. System Overview

Issuers create and sign credentials for passengers, committing sensitive attributes in a form compatible with the corresponding Circom circuit inputs. Credential schemas and per-issuer revocation entries are anchored on the consortium ledger; full credential content never leaves the passenger's device. At a checkpoint, the passenger's wallet generates a zk-SNARK proof bundle demonstrating that applicable policies are satisfied—age, nationality, document validity—and transmits it to the verifier over BLE or NFC. The verifier retrieves verification keys and revocation status from the ledger and executes a local proof check, producing an Allow or Deny decision without ever accessing raw passenger attributes. Passenger DIDs are never stored on-chain; the ledger holds only issuer-level data and aggregated revocation registries.

3.3. Threat Model

Three adversarial classes are considered. An **External Adversary** attempts to forge credentials, construct fraudulent proofs for unsatisfied policies, or replay valid proof bundles. Groth16 soundness

 doi:10.20944/preprints202604.1543.v1

prevents forgery; nonce-based freshness enforcement defeats replay. A **Malicious Verifier** seeks to extract PII from proof sessions or reconstruct travel patterns by correlating successive verifications. Since verifiers receive only Boolean policy outputs, there is no PII to extract from a well-formed proof bundle; randomized proof encodings and per-session nonces suppress cross-session linkability. **Colluding Consortium Members** attempt to combine on-chain queries with off-chain data to re-identify passengers. The structural absence of passenger DIDs from the ledger limits what colluding members can observe. Denial-of-service threats against the Fabric network are considered out of scope for this work.

4. Circom zk-SNARK Design and BIPV Architecture

Table 1 presents the BIPV layered system architecture, comprising four layers from the consortium blockchain trust anchor through user-facing interfaces.

Table 1. BIPV layered system architecture.

Layer	Component
Layer 4—User Interface	Passenger Mobile Wallet (React Native) ǀ Verifier App (Desktop/Embedded)
Layer 3—ZK Proof Engine	Circom 2.x Circuits → Groth16 zk-SNARKs (snarkjs) → Proof Cache → BLE/NFC Channel
Layer 2—Identity & Credential	DID Management ǀ Verifiable Credentials ǀ Selective Disclosure ǀ Revocation Registry
Layer 1—Consortium Blockchain	Hyperledger Fabric 2.x ǀ Airline Org ǀ Airport Authority ǀ Border Control ǀ Governance Committee

4.1. Consortium Governance and DID Layer

Airlines, airport operators, and government agencies collectively deploy a Hyperledger Fabric network with one or more channels dedicated to identity management. Each member organization runs its own peer nodes and Certificate Authority under a governance framework covering admission criteria, key rotation schedules, policy update procedures, and dispute resolution. Issuer and verifier DIDs, associated public keys, service endpoints, and revocation list references are written to ledger state via chaincode. Credential schemas and verification policies—specifying required attributes, permitted cryptographic curves, and acceptable SNARK parameters—are stored as ledger elements and referenced by identifier during proof verification, allowing governance committee updates to take effect without modifying the core verification protocol.

4.2. Credential Issuance Protocol

Credential issuance proceeds through four stages. During **Enrollment**, the passenger undergoes out-of-band KYC verification with an issuer, binding their DID and public key to a real-world identity; this binding is not recorded on the ledger. In **Credential Creation**, the issuer assembles a Verifiable Credential containing the passenger's attributes—name, date of birth, nationality, document number, validity period—and commits sensitive fields using cryptographic commitments aligned with the Circom circuit definitions. **On-chain Anchoring** records a credential hash and a new revocation registry entry on the Fabric ledger; the full credential content remains in the passenger's wallet. During **Wallet Storage**, the React Native application persists the credential, pre-computed commitments, and the circuit parameters needed for subsequent proof generation.

4.3. Circom Circuit Library for Airport Policies

 doi:10.20944/preprints202604.1543.v1

BIPV defines three Circom circuits covering the core airport policy predicates. The **AgeVerifier** circuit accepts as private inputs the committed date-of-birth and current date, computes the difference using fixed-point arithmetic, and outputs a single Boolean indicating compliance with the age threshold. The **NationalityChecker** circuit implements a set-membership proof over an allowed-country bit-vector using a Merkle inclusion argument, revealing only whether the passenger's nationality belongs to the permitted set. The **DocumentValidator** circuit verifies that the credential validity timestamp is within range and that the corresponding revocation registry entry is absent, using a sparse Merkle tree inclusion proof anchored on the Fabric ledger.

Each circuit accepts private inputs—the committed credential attributes held in the passenger's wallet—and produces public outputs consisting of Boolean compliance indicators and a Groth16 proof π. Circuits are compiled with Circom 2.x to R1CS constraint systems. A Powers-of-Tau trusted setup generates the proving and verification key pair; proving keys are distributed to passenger wallets at credential issuance, and corresponding verification keys are anchored on the Fabric ledger as chaincode state, enabling governance committee key rotations to propagate automatically to all verifiers.

4.4. Proof Pre-Computation and Caching Strategy

The Groth16 prover runs on the passenger's smartphone during check-in or while waiting in queue—not at the gate. The resulting proof bundle, containing the Groth16 proof π, public signals σ, policy references ϱ, and a per-session nonce slot η, is cached in the wallet's local secure storage for the travel day. A cache validity window is enforced: bundles are invalidated when a revocation query signals a credential status change, or when applicable policies are updated on-chain via a ledger event subscription. On a cache hit, the wallet's contribution to end-to-end latency is approximately 0.05 s—dominated by BLE or NFC transmission rather than cryptographic computation.

4.5. Checkpoint Verification Protocol

Table 2 details the seven-step verification sequence at a checkpoint. The gate broadcasts a policy request carrying policy identifiers and verification key identifiers via QR code or NFC. The wallet parses the request, checks its proof cache, and either serves a cached bundle or invokes the Circom prover for a fresh proof. The resulting bundle is sent to the verifier. The verifier queries the Fabric ledger for the relevant verification keys, issuer public keys, and current revocation status; performs a local Groth16 proof verification; and issues an Allow or Deny decision. The event log retains only the policy identifier, the issuer DID, and a timestamp—no passenger attribute is recorded.

Table 2. Checkpoint verification sequence. All PII remains on the passenger's device throughout; only Boolean policy outputs and minimal metadata cross the verification channel.

Step	Actor	Action / Message
1	Verifier Gate	Broadcasts QR/NFC policy request carrying Policy IDs and VK IDs
2	Passenger Wallet	Parses request; checks proof cache for matching policies
3	Passenger Wallet	Generates fresh Circom Groth16 proofs via snarkjs on cache miss
4	Passenger Wallet	Sends proof bundle ($\pi + \sigma + \varrho + \eta$) over BLE/TLS channel
5	Verifier Gate	Queries Hyperledger Fabric for VKs, issuer PKs, and revocation status
6	Verifier Gate	Verifies Groth16 proofs, credential freshness, and revocation status

 doi:10.20944/preprints202604.1543.v1

7	Verifier Gate	Grants or denies access; logs Policy ID, Issuer DID, and Timestamp only

5. Implementation and Evaluation

5.1. Prototype Implementation

The BIPV proof-of-concept spans four integrated components. The **blockchain layer** comprises a Hyperledger Fabric 2.x network with three organizations—Airline, Airport Operator, and Border Authority—each running peer nodes and a Certificate Authority, linked via a dedicated identity management channel. Smart contracts written in Go and Node.js handle credential schema registration, revocation registry management, verification key publication, and policy enforcement. The **ZKP layer** uses Circom circuits compiled to Groth16-compatible R1CS constraint systems, with the snarkjs library performing proof generation on both Android and iOS devices representative of typical passenger hardware. The **mobile wallet** is a React Native application supporting DID management, credential storage, Circom proof generation, and QR/NFC interactions. **Verifier software** runs on both desktop machines and embedded gate hardware, using the Hyperledger Fabric SDK to retrieve verification keys and revocation data and to execute the local Groth16 proof check.

5.2. Experimental Setup

The Fabric network ran on Docker containers hosted on commodity servers configured with one orderer node and three peer nodes. Circom proof benchmarks were conducted on mid-range Android and iOS smartphones representing a realistic cross-section of international traveller device capabilities. Four metrics were measured across 1,000 simulated verification sessions: (i) verification latency—elapsed time from proof bundle receipt to access decision; (ii) throughput—passengers processed per hour at a single checkpoint under continuous load; (iii) PII Exposure Index—count of unique directly-identifying attributes disclosed to verifiers per journey; and (iv) resource utilization on verifier nodes and the Fabric network. Results were compared against two baselines: a conventional centralized database system exposing full attributes at each touchpoint, and a DID-only system presenting signed credentials without zk-SNARK selective disclosure.

5.3. Performance Results

Table 3 presents the headline metrics. BIPV achieved a mean verification latency of 0.42 s for a standard policy bundle covering age verification, nationality check, and boarding pass validity. Under continuous operation this corresponds to approximately 2,380 passengers per checkpoint per hour, compared with 1,150 for the DID-only system and 746 for the centralized baseline. The centralized system's lower throughput reflects database round-trips required at each touchpoint; BIPV's pre-computed and cached proofs reduce verifier-side computation to a single Groth16 verification completing in under 50 ms. When a cached proof was available, the wallet's contribution to end-to-end latency fell to approximately 0.05 s.

Table 3. Performance comparison: BIPV vs. baselines. Values are averages over 1,000 verification sessions in a controlled prototype environment.

Metric	BIPV (Proposed)	DID-only	Centralized
Avg. Verification Latency	0.42 s	0.87 s	1.34 s
Throughput (passengers/hr)	2,380	1,150	746
PII Attributes Disclosed	0 (Boolean only)	5–7 avg.	10–12 avg.

 doi:10.20944/preprints202604.1543.v1

PII Reduction vs. Centralized	94.7%	~38%	Baseline
On-chain Queries per Verification	1–2 (cached)	3–4	N/A
Mobile Proof Generation (cached)	~0.05 s	N/A	N/A

5.4. PII Exposure Analysis

The PII Exposure Index counts unique directly-identifying attributes disclosed to verifiers during a complete four-touchpoint journey. Under BIPV, verifiers receive only Boolean policy outputs—*age ≥ 18: TRUE*, *nationality permitted: TRUE*—along with non-identifying metadata such as the issuer DID and a session timestamp. No name, date of birth, document number, or biometric data crosses the verification channel at any point. This reduces PII exposure by 94.7% compared to the centralized baseline, which exposes between 10 and 12 attributes at each of four touchpoints. Table 4 breaks down disclosure by touchpoint across all three systems.

Table 4. PII exposure comparison per journey touchpoint. BIPV limits disclosure to Boolean policy outcomes at every checkpoint, eliminating direct PII exposure.

Touchpoint	Centralized	DID-only	BIPV
Check-in Desk	Name, DOB, Passport, Nationality, Visa	Pseudo-DID, Name, Nationality	Booking Valid = TRUE
Security Gate	Full PII repeated	Name, DOB, Nationality, Risk Score	Cleared = TRUE
Boarding Gate	Full PII + flight details	Name, Boarding Pass ID	Authorized = TRUE
Border Control	Passport, Visa, Biometrics	DOB, Nationality, Visa Status	Age OK + Nationality OK = TRUE

6. Security and Compliance Analysis

6.1. Credential Forgery Resistance

Every issuer public key is anchored in the Fabric consortium ledger under the collective endorsement of consortium members. A credential lacking a valid issuer signature is rejected during proof generation on the wallet, since the Circom circuit will not produce a valid proof for a commitment that does not open to a properly signed value. At the verifier, Groth16 soundness—grounded in the hardness of the discrete logarithm problem and the knowledge-of-exponent assumption—ensures that an adversary cannot fabricate a valid proof for a policy predicate they do not actually satisfy.

6.2. Replay Attack Prevention

Each proof bundle incorporates a verifier-supplied ephemeral nonce η and a timestamp embedded in the public signal set σ. Policy definitions enforce a freshness window: any bundle whose nonce does not match the current verifier challenge, or whose timestamp falls outside the validity period, is unconditionally rejected. Capturing and resubmitting a legitimate bundle at a later gate or on a different travel day therefore fails without any additional application-layer mechanism.

6.3. Collusion Resistance and Linkability Reduction

 doi:10.20944/preprints202604.1543.v1

Because passenger DIDs are absent from the ledger, colluding consortium members querying on-chain state obtain only issuer-level public keys, revocation entries, and aggregate policy statistics—none of which directly identifies individual passengers. At the protocol layer, randomized proof encodings and one-time per-session nonces make two proof bundles from the same passenger computationally unlinkable to an observer seeing only transmitted data.

6.4. GDPR Compliance

BIPV was designed with four GDPR principles as explicit architectural constraints. **Data minimization** is satisfied by the Boolean-only disclosure model. **Purpose limitation** is enforced at the circuit level, since each Circom circuit encodes a specific policy purpose and cannot be repurposed to extract raw attributes without recompiling the circuit. **Storage limitation** is achieved by confining long-term PII to issuers and passenger devices; the ledger retains only hashes and revocation entries. **Data subject rights** are supported through the credential revocation mechanism and through the wallet's proof selection interface.

6.5. Alignment with ICAO Annex 17 and IATA One ID

ICAO Annex 17 mandates reliable passenger identification and secure handling of travel documents [12]. BIPV meets the identification requirement through cryptographically sound credential verification while limiting document detail exposure to the minimum needed for a decision. IATA One ID envisions a model in which a passenger's digital identity is validated once and reused across touchpoints without repeated PII disclosure [14]. BIPV operationalizes this vision: pre-computed proof bundles generated at home or during check-in can be presented at every subsequent security and boarding checkpoint.

7. Discussion

7.1. Limitations

Several limitations merit acknowledgment. The prototype assumes passengers carry smartphones capable of executing Groth16 proof generation within a reasonable time window; passengers without compatible devices require assisted verification flows or fallback document checks, which reintroduce some PII exposure. Our evaluation was conducted in a controlled laboratory environment simulating load patterns; a live airport introduces physical environment variability, intermittent network conditions, and human factors that our trials did not capture. Although BIPV dramatically reduces PII exposure at checkpoints, issuers and some consortium members necessarily retain sensitive credential data and must apply strong internal security controls independently of the BIPV architecture. Resilience of the Fabric network to sustained high-volume traffic or coordinated denial-of-service pressure at peak airport loads remains an open question for dedicated follow-on study.

7.2. Deployment Considerations

Translating BIPV from a prototype to a production airport system requires attention to several dimensions beyond technology. Legal and governance agreements must allocate liability, define data retention obligations for on-chain records, and specify procedures for member admission and revocation. Integration with airline reservation systems, boarding control platforms, and real-time risk assessment databases would need to be redesigned so that risk signals reach verifiers without flowing through PII-bearing channels. User experience design deserves particular emphasis: the wallet interaction must be straightforward enough that first-time international travellers can complete it quickly, and accessibility accommodations must be available for passengers who cannot operate a smartphone. A phased rollout in which BIPV checkpoints operate in parallel with legacy document checks during a transition period is likely to be both practically and politically necessary.

 doi:10.20944/preprints202604.1543.v1

7.3. Generalization Beyond Aviation

The core BIPV model—Circom zk-SNARKs for selective disclosure, DID-anchored credentials, consortium blockchain for shared trust—applies to any domain requiring high-assurance, high-throughput identity verification under privacy obligations. Candidate domains include border crossings, large-scale event venues, critical infrastructure access control, and healthcare credentialing. Future work will evaluate hardware-accelerated proof generation for resource-constrained devices, formal verification of the Circom circuits using the Lean theorem prover, and extension of the threat model to cover denial-of-service resilience.

8. Conclusions

This paper has presented BIPV, a blockchain-based identity and privacy verification framework that integrates W3C Decentralized Identifiers, Circom-compiled Groth16 zk-SNARKs, and a Hyperledger Fabric consortium blockchain to enable privacy-preserving airport passenger screening at operationally meaningful throughput. Our prototype demonstrates that secure identity verification does not require sharing complete personal data: by reducing checkpoint disclosure to Boolean policy outcomes, BIPV achieves a 94.7% reduction in PII exposure relative to centralized baselines while maintaining a mean verification latency of 0.42 s and sustaining 2,380 passengers per checkpoint per hour.

Security analysis confirms resistance to credential forgery, replay attacks, and consortium collusion under standard cryptographic assumptions. The design satisfies GDPR data minimization requirements and aligns with both ICAO Annex 17 and IATA One ID guidelines, making it a credible candidate for regulatory acceptance alongside technical adoption. Beyond aviation, the BIPV model provides a generalizable template for privacy-preserving, high-throughput identity verification in any domain subject to data protection obligations.

Author Biographies

AARADHYA PATANGIYA received her B.Tech degree in Computer Science and Engineering from SRM Institute of Science and Technology, Kattankulathur, India. Her research interests include blockchain-based privacy-preserving systems, zero-knowledge proofs, decentralized identity management, and applied cryptography. She is a student member of IEEE.

DR. AROKIARAJ JOVITH A is an Associate Professor in the Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, India. He received his Ph.D. in Computer Science and Engineering. His research interests include distributed systems, blockchain technology, network security, and privacy-enhancing technologies. He is a senior member of IEEE. Correspondence: arokiara@srmist.edu.in.

Author Contributions: Conceptualization, A.P. and A.J.A.; methodology, A.P.; software, A.P.; validation, A.P. and A.J.A.; formal analysis, A.P.; investigation, A.P.; writing—original draft preparation, A.P.; writing—review and editing, A.J.A.; visualization, A.P.; supervision, A.J.A.; project administration, A.J.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors acknowledge the support of the Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur.

Conflicts of Interest: The authors declare no conflicts of interest.

References

 doi:10.20944/preprints202604.1543.v1

1. Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed on 1 January 2025).
2. W3C. Decentralized Identifiers (DIDs) v1.0. W3C Recommendation, July 2022. Available online: https://www.w3.org/TR/did-core/ (accessed on 1 January 2025).
3. W3C. Verifiable Credentials Data Model v1.1. W3C Recommendation, March 2022. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 1 January 2025).
4. Hyperledger. Identity—Hyperledger Fabric Documentation v2.5. Available online: https://hyperledger-fabric.readthedocs.io/ (accessed on 1 January 2025).
5. IEEE. IEEE Editorial Style Manual; IEEE Author Center: Piscataway, NJ, USA, 2023.
6. Chen, H.-Y.; et al. An International Federal Hyperledger Fabric Verification Framework of Digital Vaccine Passport. *Int. J. Environ. Res. Public Health* 2022, *19*, 1757. https://doi.org/10.3390/ijerph19031757
7. Author, A. Proofs and ZK-SNARKs Circuits with Circom ZK and Iden3 Protocol. *IJIRT* 2024, *11*, 45–52.
8. Dock. Circom Integration: Anonymous Credentials Protocol Update. 2025. Available online: https://www.dock.io (accessed on 1 January 2025).
9. Author, X. ID-based Self-encryption via Hyperledger Fabric Based Smart Contract. *arXiv* 2022, arXiv:2207.01605.
10. European Parliament. General Data Protection Regulation (GDPR). *Official Journal of the European Union*, April 2016.
11. Author, Y. ZAPS: A Zero-Knowledge Proof Protocol for Secure UAV Flight Path Verification. *arXiv* 2025.
12. ICAO. Annex 17 to the Convention on International Civil Aviation—Security, 11th ed.; ICAO: Montreal, QC, Canada, 2020.
13. Author, Z. Biometric Systems in Philippine Airports: Balancing Security and Privacy. *IJARSCT* 2023, *3*, 12–21.
14. IATA. One ID: A Transformative Passenger Journey Concept; IATA: Montreal, QC, Canada, 2023.
15. International Security Journal. Highlighting the Weak Links in Airport Identity Security, February 2026.