Licensing/Commercialisation Opportunity

PCT-IN23-0941: System and Method for Facilitating Decentralized Identity Management

Secure, Privacy-First, and Interoperable Identity Solution for the Future

About The Patent

PATENT NO. PCT-IN23-0941

- **Applicant and Inventor:** Amit Dua .
- **Additional Inventors:** Arijeet Sengupta and Ipshita Mahapatra.
- **Filing Date:** June 16, 2023 (priority claim from Indian application 202311041001).
- **International Filing:** Processed under the Patent Cooperation Treaty (PCT) via the International Bureau of WIPO.

1. INTRODUCTION:

The digital world demands secure, private, and user-friendly identity management solutions. Patent PCT-IN23-0941 introduces a groundbreaking system and method for decentralized identity management, leveraging biometric authentication, zero-knowledge proofs (ZKPs), and decentralized storage to address the limitations of traditional centralized systems. This deck outlines the patents technology, benefits, market potential, and commercialization opportunities for prospective buyers or licensors.

1.1 PROBLEM ADDRESSED:

Centralized identity management systems suffer from: •

Data Breaches: Centralized databases are prime targets for hackers.

Single Point of Failure: A breach in the central authority disrupts the entire system.

Lack of User Control: Users have limited say over their personal data.

Limited Interoperability: Systems often lack compatibility across platforms.

Inefficient Authentication: Complex passwords and processes frustrate users.

Existing solutions like federated identity management, standalone ZKPs, or privacyenhancing technologies (e.g., differential privacy) only partially address these issues, often lacking comprehensive privacy or user-friendliness.

1.3 SOLUTION OFFERED

Patent PCT-IN23-0941 provides a decentralized identity management system that:

- Uses biometric data (e.g., fingerprints, facial recognition, iris scans) for secure authentication. •
- Employs zero-knowledge proofs to verify identities without revealing sensitive data.
- Stores data in decentralized networks (e.g., blockchain, Filecoin, Storj) for enhanced security and user control.
- Enables seamless interoperability across platforms, promoting a connected identity ecosystem.

2. HOW IT WORKS

The system (denoted as system 102) comprises processors, memory, and specialized modules to deliver secure and private identity management.

2.1 SYSTEM ARCHITECTURE

Data Acquisition Module: Collects biometric data from user devices (e.g., smartphones, IoT devices).

Identity Generation Module: Converts biometric data into a secure digital template using SHA-256 hashing to create a Biometric Identity (ID). Generates a Decentralized Identification Number (DID) and stores their mapping.

Zero-Knowledge Proof Module: Creates and verifies ZKPs based on the Biometric ID-to-DID mapping, ensuring authentication without exposing data.

Authentication Module: Verifies ZKPs and grants access to services while maintaining user privacy.

2.2 METHOD FLOW

1. Receive Data: The system receives biometric data (e.g., fingerprint, iris scan) from a users device.

2. Store Data: Data is stored in a decentralized network, enabling user control.

3. Generate ZKP: A zero-knowledge proof is created based on the hashed biometric data and DID mapping.

4. Verify and Grant Access: The ZKP is verified without accessing the underlying data, granting access to the requested service upon successful verification.

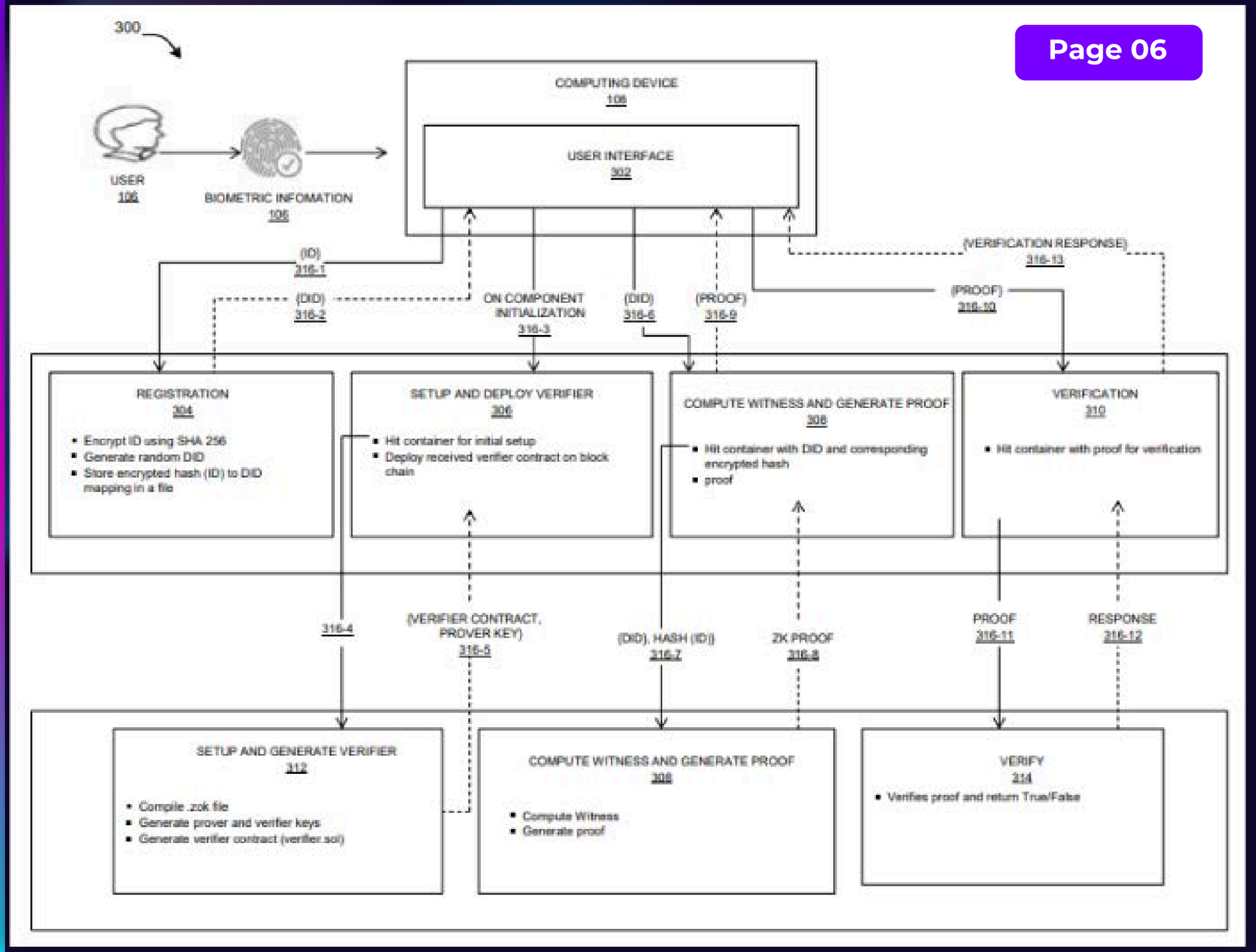
2.3 PROCESS EXAMPLE

When a user registers, their biometric data is hashed using SHA-256 to create a Biometric ID, paired with a DID, and stored in a decentralized network. During authentication, a ZKP is generated and verified, allowing access to services without exposing the biometric data. This process is illustrated in the patents figures (e.g., FIG. 3), showing registration, ZKP generation, and verification steps.

IIPRD

2.4 PROCESS EXAMPLE

When a user registers, their biometric data is hashed using SHA-256 to create a Biometric ID, paired with a DID, and stored in a decentralized network. During authentication, a ZKP is generated and verified, allowing access to services without exposing the biometric data. This process is illustrated in the patents figures (e.g., FIG. 3), showing registration, ZKP generation, and verification steps.



3. Benefits for Buyers or Licensors

This patent offers significant advantages for companies looking to acquire or license it:

Enhanced Security: Decentralized storage reduces the risk of data breaches compared to centralized systems.

Privacy Preservation: Users authenticate without revealing sensitive biometric data, aligning with privacy expectations.

Interoperability: Enables seamless identity verification across platforms, fostering a connected digital ecosystem.

User Control: Empowers users to manage their identity data, deciding what to share and with whom.

User-Friendly: Eliminates complex passwords, simplifying authentication for endusers.

Regulatory Compliance: Supports GDPR and other data protection laws by prioritizing user rights and privacy.

4. MARKET POTENTIAL

The decentralized identity market is poised for explosive growth, driven by increasing demand for secure and user-centric identity solutions.

4.1 MARKET SIZE & GROWTH

The decentralized identity market is projected to reach USD 72.35 billion by 2033, with a CAGR of 90.8% (Emergen Research).

Growth is fueled by rising security breaches, inefficiencies in centralized systems, and demand for user-controlled identities.

4.2 KEY MARKET DRIVERS

Security Breaches: Increasing instances of identity-related fraud drive demand for secure solutions.

User Control: Consumers demand greater control over their personal data.

Inefficient Systems: Centralized systems are cumbersome and vulnerable.

Industry Applications: Extensive use in banking, cybersecurity, IoT, and more.

Self-Sovereign Identity (SSI): Growing adoption of SSI frameworks enhances market potential.

4.3 TARGET SECTORS

BFSI: Secure authentication for banking, payments, and KYC processes.

Government: Digital identity solutions for public services and resident cards.

Healthcare: Protecting patient data while enabling secure access.

Telecom & IT: Authentication for IoT and smart devices

Retail & E-commerce: Seamless customer verification across platforms

4.4 MARKET TRENDS

Blockchain Integration: Blockchain is at the forefront of decentralized identity solutions.

Zero-Knowledge Proofs: ZKPs are a breakthrough for privacy-preserving authentication.

Self-Sovereign Identity: SSI frameworks empower users to manage their identities independently.

Digital Transformation: The shift to digital services (accelerated by COVID-19) amplifies the need for reliable identity systems.

5. GDPR & REGULATORY COMPLIANCE

The patent aligns seamlessly with global data protection regulations, making it an attractive solution for compliance-conscious organizations.

5.1 GDPR ALIGNMENT

Data Minimization: Users share only necessary data via ZKPs, complying with GDPRs principle of minimal data processing.

User Rights: Supports GDPR rights like access, rectification, and deletion by giving users control over their data.

Privacy by Design: The system embeds privacy measures into its architecture, aligning with GDPRs Privacy by Design and by Default requirement (Medium: GDPR Compliance).

5.2 GLOBAL APPLICABILITY

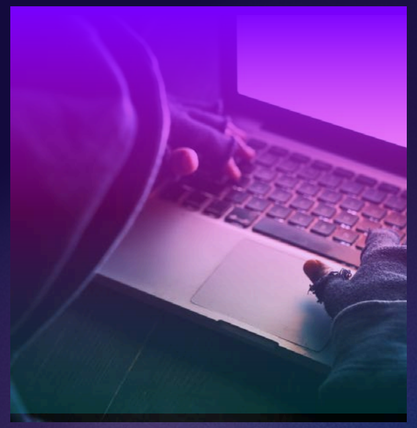
The system can be adapted to other regulations like the California Consumer Privacy Act (CCPA) and Brazils General Data Protection Law (LGPD) (IDPro: GDPR Impact).

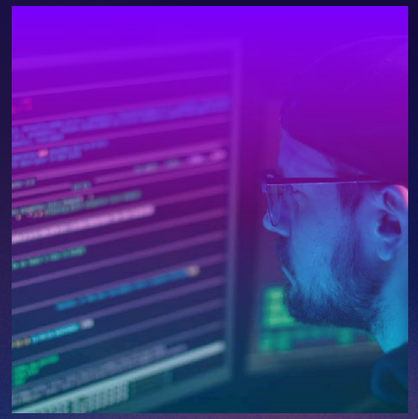
Decentralized identity reduces compliance risks by minimizing centralized data storage.

5.3 REGULATORY BENEFITS

Enables organizations to demonstrate compliance through transparent, user-controlled data handling.

Reduces the need for repeated identity checks, streamlining compliance with KYC and AML regulations (Togggle: GDPR and Blockchain).





COMPETITIVE LANDSCAPE

KEY PLAYERS, DIFFERENTIATION, PATENT STRENGTH

KEY PLAYERS:
SecureKey Technologies Inc., Avast Software s.r.o., Civic Technologies, Inc., and others are active in the market (Grand View Research).

Microsofts Entra includes decentralized identity solutions, indicating industry interest (Grand View Research: IAM).

DIFFERENTIATION:
Unique Integration: Combines biometric authentication, ZKPs, and decentralized storage in a single system. •

Comprehensive Solution: Unlike standalone ZKP or federated identity systems, it addresses security, privacy, and interoperability holistically.

User-Centric: Prioritizes user control and privacy, aligning with consumer demands.

PATENT STRENGTH:
Novel combination of technologies addresses multiple identity management challenges.

Offers a scalable, adaptable framework for various industries and use cases.

MONETISATION STRATEGIES

The patent offers multiple avenues for commercialization, providing flexibility for buyers or licensors.

Product Development: Develop standalone decentralized identity management solutions for sale to enterprises or consumers.

Service Offering: Provide identity verification services via a Software-as-a-Service (SaaS) platform, leveraging the patented technology.

Licensing: License the patent to companies in identity management, blockchain, or biometric technology sectors.

Partnerships: Collaborate with blockchain platforms (e.g., Ethereum, Hyperledger), biometric technology providers, or identity management firms to integrate the technology.

IIPRD

WHY CHOOSE US?

This patent is a strategic asset for companies aiming to lead in the digital identity space.

First-Mover Advantage: Enter a rapidly growing market with a patented, innovative solution, positioning your company as a leader.

Innovative Technology: Combines cutting-edge biometric authentication, ZKPs, and decentralized storage for a unique value proposition.

Regulatory Compliance: Ready-made solution for GDPR, CCPA, and other regulations, reducing compliance risks and costs.

Scalability: Applicable across industries (BFSI, healthcare, government, etc.) and use cases, ensuring broad market appeal.

User-Centric Design: Focuses on user privacy and control, aligning with growing consumer demands for data sovereignty.

Trust-Building: Provides a foundation for building trust in digital interactions, crucial in todays data-driven world.

Call to Action:

Explore partnership opportunities to bring this cutting-edge technology to market. Contact us to discuss licensing, development, or collaboration possibilities.

Contact: +91 98106 17992 - Mail: Tarun@iiprd.com - Visit: www.iiprd.com