NON-PROVISIONAL PATENT APPLICATION

Title: ZERO-KNOWLEDGE VERIFICATION OF HEALTH DATA USING CRYPTOGRAPHIC PROOFS

Inventor: Michael E Hollins Jr Address: 56 Beaver St., Apt. 205, New York, NY 10004 USA

Cross-Reference to Related Applications: None

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to privacy-preserving cryptographic verification systems withi

Description of Related Art

Current health verification systems face a fundamental privacy paradox: proving health data

Existing solutions suffer from critical technical limitations: (1) Direct Data Sharing syste

Performance analysis reveals existing systems achieve verification throughput of only 10-50

No existing system provides mathematical certainty of health goal compliance (e.g., "achieve

SUMMARY OF THE INVENTION

The present invention introduces a system for cryptographic verification of health data tha

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1: Zero-Knowledge Health Verification System Architecture
Figure 2: Zero-Knowledge Constraint Satisfaction Circuit Architecture

DETAILED DESCRIPTION OF THE INVENTION

The zero-knowledge health verification system comprises four main components:

First, a Health Data Aggregation Module that collects data from multiple health platforms (A

Second, a Cryptographic Proof Generator that implements custom zk-SNARK circuits for health

Third, a Blockchain Storage Layer that stores cryptographic proofs on immutable distributed

Fourth, a Verification API Framework that provides interfaces for third-party verification,

The system employs custom constraint circuits specifically designed for health data verifica

Performance specifications include: proof generation time of 50-200 milliseconds per health

CLAIMS

1. A computer-implemented method for privacy-preserving verification of personal biometric information using cryptographic proofs, comprising: collecting verified personal health information from multiple trusted data sources including wearable devices, mobile applications, and healthcare systems on a user's computing device; generating a zero-knowledge cryptographic proof employing constraint satisfaction circuits that validate the personal health information against configurable verification criteria; the circuits are configured to adapt dynamically based on user demographic profiles and data source reliability metrics; storing the cryptographic proof on a blockchain-based distributed system to facilitate public verification while preserving data privacy; and providing a verification interface for third parties to cryptographically confirm compliance with specified criteria without access to or disclosure of the underlying personal health information.

2. The method of claim 1, wherein the biological and temporal constraints implemented by the circuits include physiologically feasible ranges for metrics such as heart rate, sleep duration, and blood pressure, adjusted based on user age, gender, and health profile.

3. The method of claim 1, wherein the cryptographic proof incorporates cryptographic commitments to health data and device reliability scores, enabling verifiers to confirm proof authenticity without revealing specific measurement data.

4. The method of claim 1, wherein the constraint satisfaction circuits support hierarchical validation workflows, requiring proof of prerequisite health conditions—such as vaccination status or baseline health metrics—before endorsing more complex health data tokens or certifications.

5. The method of claim 1, further comprising anomaly detection algorithms that filter or flag inconsistent or suspicious health data prior to proof generation, thereby improving the reliability and trustworthiness of the cryptographic attestations.

6. The method of claim 1, wherein the proof generation supports batch processing, allowing multiple health data proofs to be generated and verified simultaneously while maintaining privacy guarantees for each individual proof.

7. The method of claim 1, wherein the cryptographic proofs include secure timestamps and time-lock guarantees, attesting to the sustained compliance over specific periods, supporting verification for periodic or ongoing health behaviors.

8. The method of claim 1, wherein the cryptographic proof scheme employs zero-knowledge cryptographic protocols including zk-SNARKs, zk-STARKs, or other succinct proof systems optimized for minimal proof size and fast verification, suitable for scalable, real-time biometric data

verification across multiple platforms and devices.

9. The method of claim 1, wherein the system automatically incorporates regulatory compliance features—including GDPR and HIPAA—such as data erasure, right-to-portability, and cryptographic proof invalidation, into the proof generation workflow.

10. A distributed cryptographic verification system for personal biometric information, comprising: a local data aggregation component that collects biometric measurements from multiple data sources including wearable devices, mobile applications, and connected health platforms; a cryptographic proof engine configured to generate privacy-preserving verification proofs utilizing configurable constraint validation and temporal verification logic; a distributed ledger interface that stores cryptographic proofs in an immutable and publicly verifiable manner across multiple blockchain protocols; and a verification framework enabling third-party confirmation of proof validity without accessing or revealing underlying personal biometric information, all configured to support multi-jurisdictional regulatory compliance and data privacy requirements.

11. The system of claim 10, wherein the proof engine employs adaptive constraint circuits that incorporate demographic data, device accuracy scores, and device reliability metrics.

12. The system of claim 10, further comprising a trusted execution environment or secure enclave that performs on-device proof generation, ensuring raw health data remains private and local.

13. The system of claim 10, wherein the blockchain interface supports interoperability across multiple blockchain protocols, allowing health data tokens and proofs to be verified on different distributed ledgers.

14. The system of claim 10, wherein the proof validation process involves cryptographic commitments combined with compliance flags such as consent status and regulatory flags, integrated into the stored proofs.

15. The system of claim 10, wherein the API framework supports multi-stakeholder workflows, including patient control, healthcare provider validation, insurer verification, and regulatory audit.

16. The system of claim 10, wherein the cryptographic proofs are capable of supporting the right to erasure and data portability through cryptographic invalidation or proof revocation mechanisms, compliant with GDPR policies.

17. The system of claim 10, wherein the proof engine employs anomaly detection and machine learning algorithms to improve confidence scores, filtering out inconsistent or suspicious health data prior to proof creation.

18. The method of claim 1, wherein the health data aggregation includes rate

limiting of 1-1000 API calls per minute per platform to prevent data harvesting attacks while maintaining real-time synchronization.

19. The method of claim 1, wherein the zero-knowledge circuit includes range proofs that ensure health measurement values fall within medically validated ranges, such as 0-100,000 steps per day, heart rate between 40-220 BPM, sleep duration between 0-24 hours per day, with automatic rejection of biologically impossible values.

20. The method of claim 1, wherein the cryptographic proof generation includes temporal sequence validation ensuring biometric data timestamps are chronologically ordered and fall within configurable time windows, preventing replay attacks and stale data injection while supporting real-time verification requirements with sub-second latency guarantees.

ABSTRACT

A novel system and method for cryptographic verification of health data, enabling privacy-pr