PROVISIONAL PATENT APPLICATION: CLOUD COMPUTING, DATA OPTIMIZATION, & DECENTRALIZED SECURITY

Invention Title: SYSTEM AND METHOD FOR RECURSIVE SEMANTIC SANITIZATION, GLOBAL REDUNDANCY EXTRACTION, ZERO-KNOWLEDGE USER PRIVACY, AND CIRCULAR HARDWARE REPURPOSING IN CLOUD ARCHITECTURES

First Named Inventor: * Given Name(s): John Lawrence

Family Name: Coulson

City of Residence: Whistler

State/Province: British Columbia

Country: Canada V8E 1N7

Correspondence Address: * Name: John L. Coulson

Address: Suite 201 - 1330 Cloudburst Drive

City: Whistler

State/Province: BC

Country: Canada V8E 1N7

Email: jlc@sidogger.com

Entity Status: "Micro Entity"

U.S. Government Agency Interest: NO.

1. The Field of Invention

This invention relates to the field of data storage optimization, zero-knowledge decentralized security, environmental sustainability, and circular hardware economies within cloud computing infrastructure. Specifically, it addresses the global "dark data" crisis inherent in distributed electronic communications by utilizing Semantic DNA deduplication to radically reduce the physical hardware footprint, power consumption, and unmanaged carbon emissions of data centers, thereby circumventing the need for expansive new server facility construction.

2. The Technical Problem

Traditional data deduplication processes are computationally "blind," relying primarily on exact bit-for-bit algorithmic matches of metadata. If a user alters the metadata of a redundant file (e.g., renaming a forwarded 50 MB video attachment), the server stores a duplicate physical copy. Multiplied across billions of global users, this redundancy creates "Digital Permafrost"—vast archives of stale, duplicate data. Current data trends indicate up to 80% of stored electronic data is unaccessed for years.

Simultaneously, enterprise technology sectors are forecasting trillions of dollars in Capital Expenditure (CapEx) to construct new, high-energy data centers to accommodate this data bloat alongside emerging AI demands. This global digital landfill requires continuous, massive electrical and cooling overhead, representing a primary source of unmanaged carbon emissions and municipal power grid strain.

3. The Technical Solution: The "Medicinal Scrub" Protocol

The architecture introduces a "Medicinal Scrub" protocol utilizing an AI-driven Semantic DNA fingerprinting system. It surgically sanitizes high-energy servers through the following integrated subsystems:

Semantic DNA Diagnostics: The system bypasses surface-level metadata and analyzes the fundamental structural binary (the "DNA") of the content itself, recognizing identical files across cross-platform domains regardless of superficial alterations.

The "Ghost Pointer" Interface & Zero-Knowledge Privacy: Upon identifying semantic duplicates, the protocol extracts the multi-megabyte payloads from local servers and replaces them with a 1-KB cryptographic "Ghost Pointer." This pointer acts as a Zero-Knowledge Decentralized Access Pointer (ZK-DAP). The central server cannot read the data. To the user, the interface appears unchanged, but the file can only be decrypted locally using the user's private cryptographic key.

The 2055/3055 Cold-Storage Bunker: Verified redundant master assets are compressed using fractal algorithms and migrated to non-electrified, subterranean cold-storage installations, dropping operational storage power demands by 99.9% while preserving the historical integrity of human data records.

Trillion-Dollar CapEx Avoidance: By executing this recursive deduplication, the system reclaims vast percentages of physical server space instantly, negating the enterprise requirement to construct new data facilities and preserving global land, municipal water (for cooling), and power resources.

The "Repurpose & Donate" Circular Economy Matrix: As the Global Redundancy Extraction liberates physical server space, obsolete but functional server racks are systematically decommissioned. The central system generates an automated manifest, packaging this dormant hardware as high-capacity educational micro-servers. These units are deployed to students and communities in developing nations, turning a corporate e-waste problem into a humanitarian market expansion strategy.

4. DETAILED DESCRIPTION OF THE DRAWINGS (LOGIC FLOWCHARTS)

Flowchart 1: Semantic DNA Fingerprinting & Diagnostics

BOX 1: System initiates a localized or cross-domain diagnostic sweep of stored "Inert Data" (stale email archives, cloud drive uploads).

BOX 2: Protocol executes a deep-packet Semantic DNA scan on the file's core binary structure, bypassing traditional metadata hashing.

BOX 3 (Decision Node): Does the generated Semantic DNA match an existing master hash in the central global registry?

If NO: Asset is unique. System generates a new master hash, stores the file, and registers the fingerprint. Return to BOX 1.

If YES: File is flagged as a "Semantic Duplicate." Proceed to extraction queue.

Flowchart 2: Extraction & Ghost Pointer Injection

BOX 1: Protocol permanently purges the physical duplicate payload from the high-energy local server drive.

BOX 2: Protocol dynamically injects a 1-KB cryptographic Ghost Pointer into the user's local directory, visually maintaining the exact UI record of the file.

BOX 3 (Decision Node): Does the user attempt to open/download the scrubbed file?

If NO: Ghost Pointer remains dormant, consuming negligible space.

If YES: System utilizes the pointer to route a secure, encrypted stream from the Cold-Storage Bunker to the user's localized device for immediate on-screen re-inflation.

Flowchart 3: The Circular Hardware Repurposing Loop

BOX 1: Central Server MCU monitors total liberated disk space and computes Total Energy Reduction (TER).

BOX 2 (Decision Node): Has liberated space within a hardware cluster met the consolidation threshold?

If YES: MCU migrates remaining active data to the newest, most energy-efficient drives.

If NO: Maintain monitoring.

BOX 3: MCU severs power to the emptied older server racks, immediately halting cooling and electrical loads to bypass new facility construction.

Flowchart 4: Zero-Knowledge Decryption & Cold-Storage Retrieval This chart maps the consumer privacy fail-safe, proving the central server cannot read the user's data.

- BOX 1: User clicks or attempts to open the 1-KB cryptographic "Ghost Pointer" located in their local directory (e.g., an old email attachment).
- BOX 2: The localized application sends a secure retrieval request to the 2055/3055 Cold-Storage Bunker, presenting a Zero-Knowledge Proof (ZKP) generated by the user's private key.
- BOX 3 (Decision Node): Does the Cold-Storage Bunker verify the user's cryptographic authority to access the master asset?

o If NO: Access is instantly denied. Master asset remains symmetrically encrypted in the bunker. System logs an unauthorized access attempt.

o If YES: Proceed to BOX 4.

- BOX 4: The bunker routes the encrypted master file stream directly to the user's localized device.
- BOX 5: The user's device utilizes its localized private key to decrypt and re-inflate the file seamlessly on the screen, ensuring the central server and intermediary networks never possess readable data.

Flowchart 5: Enterprise CapEx Avoidance & Carbon Credit Minting This chart maps the financial reporting loop that prevents corporations from building new, unnecessary data centers.

- BOX 1: Central Server MCU tallies the cumulative petabytes of physical storage space liberated by the Medicinal Scrub protocol over a 30-day fiscal cycle.
- BOX 2: Protocol cross-references the liberated space against current enterprise data-growth trajectories and real estate/construction cost metrics.
- BOX 3: System automatically generates an "Infrastructure CapEx Avoidance Report," detailing the exact dollar amount saved by bypassing new physical server facility construction.
- BOX 4: System calculates the Total Energy Reduction (TER) derived from halted cooling/electrical loads of the decommissioned racks.
- BOX 5: Protocol mints verified Carbon-Reclamation Credits proportional to the TER, depositing them into the enterprise's digital ledger for carbon-offset compliance and public reporting.

BOX 4: System generates automated Carbon-Reclamation Credits based on the TER.

BOX 5: System flags intact hardware for the humanitarian pipeline, routing the physical drives for deployment in developing educational infrastructures.

5. REPRESENTATIVE CLAIMS

Claim 1: A computer-implemented method for the medicinal sanitization of distributed cloud servers, comprising: utilizing a semantic analysis engine to generate a unique content-DNA fingerprint for a data asset; identifying redundant assets across distinct domains matching said fingerprint; extracting said redundant assets; replacing said extracted assets with a localized low-weight cryptographic pointer; and calculating a Total Energy Reduction (TER) metric to generate a corresponding automated Carbon-Reclamation Credit.

Claim 2: The method of Claim 1, wherein the low-weight cryptographic pointer operates as a Zero-Knowledge Decentralized Access Pointer (ZK-DAP), ensuring central server environments possess zero readable knowledge of the user's private data payload until localized decryption occurs.

Claim 3: The method of Claim 1, further comprising the migration of a verified singular master data asset to a non-electrified subterranean cold-storage installation, accessible only via a localized, decrypted retrieval request.

Claim 4: A system for creating a circular hardware economy, wherein the attainment of predefined volumetric data thresholds achieved by the method of Claim 1 automatically triggers the systematic electrical decommissioning of legacy server hardware, bypassing new infrastructure CapEx, and generates an automated logistical manifest for the physical repurposing of said hardware for international educational deployment.