5-SecureSphere Patents 3of3 20241031
Written by: Paul Lowndes <ZeroTrust@NSHkr.com>

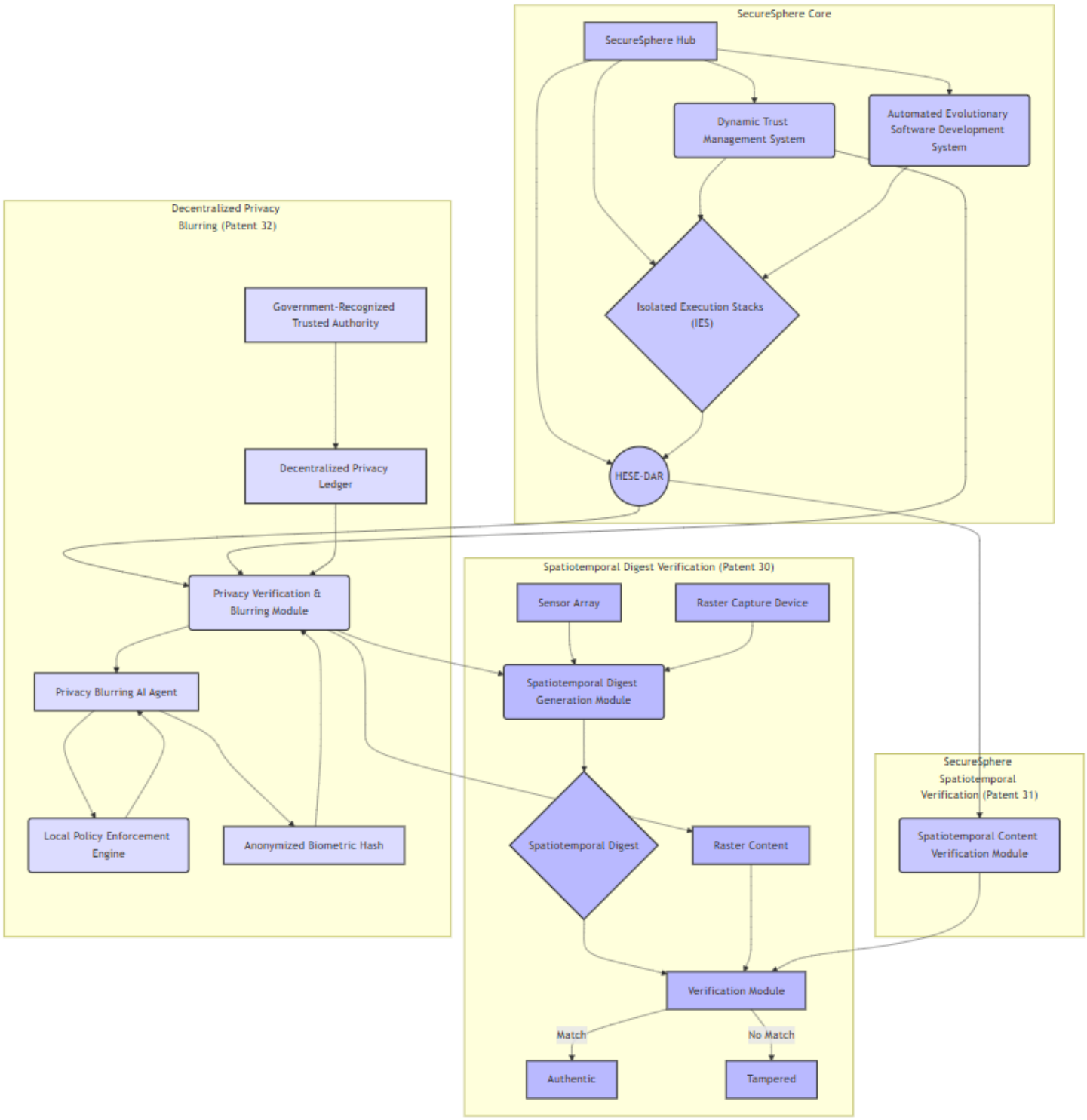
Table of Contents

Patent Group VII - MEDIA INTEGRATION

Diagram for Patent 30, 31, 32 Integration:

```
graph
    subgraph SecureSphere Core
        A[SecureSphere Hub] --> B(Dynamic Trust Management System);
        A --> C(Automated Evolutionary Software Development System);
        A --> D{"Isolated Execution Stacks (IES)"};
        A --> E((HESE-DAR));
        B --> D;
        C --> D;
        D --> E;
        style A fill:#ccf,stroke:#333,stroke-width:2px
        style B fill:#ccf,stroke:#333,stroke-width:2px
        style C fill:#ccf,stroke:#333,stroke-width:2px
        style D fill:#ccf,stroke:#333,stroke-width:2px
        style E fill:#ccf,stroke:#333,stroke-width:2px
        class A,B,C,D,E secure
    end

    subgraph "Spatiotemporal Digest Verification (Patent 30)"
        F[Sensor Array] --> G(Spatiotemporal Digest Generation Module);
        H[Raster Capture Device] --> G;
        G --> I{Spatiotemporal Digest};
        I --> J[Verification Module];
        K[Raster Content] --> J;
        J -- Match --> L[Authentic];
        J -- No Match --> M[Tampered];
        style F fill:#bbf,stroke:#333,stroke-width:2px
        style G fill:#bbf,stroke:#333,stroke-width:2px
        style H fill:#bbf,stroke:#333,stroke-width:2px
        style I fill:#bbf,stroke:#333,stroke-width:2px
        style J fill:#bbf,stroke:#333,stroke-width:2px
        style K fill:#bbf,stroke:#333,stroke-width:2px
        style L fill:#bbf,stroke:#333,stroke-width:2px
        style M fill:#bbf,stroke:#333,stroke-width:2px
        class F,G,H,I,J,K,L,M patent30
    end

    subgraph "SecureSphere Spatiotemporal Verification (Patent 31)"
        E --> N(Spatiotemporal Content Verification Module);
        N --> J;
        style N fill:#ccf,stroke:#333,stroke-width:2px
        class N patent31
    end

    subgraph "Decentralized Privacy Blurring (Patent 32)"
        O[Privacy Blurring AI Agent] --> P(Local Policy Enforcement Engine);
```

```
    P --> O;
    O --> Q[Anonymized Biometric Hash];
    Q --> R(Privacy Verification & Blurring Module);
    R --> O;
    R --> G;
    R --> K;
    E --> R;
    B --> R;
    S[Decentralized Privacy Ledger] --> R;
    T[Government-Recognized Trusted Authority] --> S;
    style O fill:#ddf,stroke:#333,stroke-width:2px
    style P fill:#ddf,stroke:#333,stroke-width:2px
    style Q fill:#ddf,stroke:#333,stroke-width:2px
    style R fill:#ddf,stroke:#333,stroke-width:2px
    style S fill:#ddf,stroke:#333,stroke-width:2px
    style T fill:#ddf,stroke:#333,stroke-width:2px
    class O,P,Q,R,S,T patent32
end

linkStyle 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 stroke:#555,stroke-width:1px

classDef secure fill:#ccf,stroke:#333,stroke-width:2px
classDef patent30 fill:#bbf,stroke:#333,stroke-width:2px
classDef patent31 fill:#ccf,stroke:#333,stroke-width:2px
classDef patent32 fill:#ddf,stroke:#333,stroke-width:2px
classDef device fill:#bbf,stroke:#333,stroke-width:2px
classDef authority fill:#ddf,stroke:#333,stroke-width:2px
classDef enclave fill:#aaf,stroke:#333,stroke-width:2px
classDef communication fill:#ccf,stroke-width:2px,stroke:#333
```



Description of Diagram for Patent 30, 31, 32 Integration

This diagram illustrates the synergistic integration of Patents 30, 31, and 32 within the SecureSphere architecture. The diagram uses color-coding to visually distinguish the components associated with each patent.

SecureSphere Core (Blue): Represents the foundational SecureSphere components including the Hub, DTMS, AESDS, IES, and HESE-DAR. The HESE-DAR acts as a central secure enclave for sensitive data processing.

Spatiotemporal Digest Verification (Patent 30, Light Blue): This subsystem focuses on verifying the authenticity of raster content based on its spatiotemporal context. The sensor array captures environment data, the digest generation module creates a digest from that data, and the verification module compares it to a recreated digest from the raster content. A match indicates the content is authentic and not altered.

SecureSphere Spatiotemporal Verification (Patent 31, Blue): This module (within the HESE-DAR) integrates with Patent 30's verification process. It leverages the spatiotemporal digest, ensuring a tamper-evident link between the raster content and the real world environment. It is essential to the privacy module, as it provides an additional way to verify the integrity of the content itself.

Decentralized Privacy Blurring (Patent 32, Light Green): This subsystem enables privacy protection. The Privacy Blurring AI Agent (on a device) identifies faces in images, performs anonymized hashing, and interacts with SecureSphere. A Local Policy Enforcement Engine helps to pre-blur data according to locally defined policies. The Privacy Verification & Blurring Module (within SecureSphere's HESE-DAR) performs identity verification against a Decentralized Privacy Ledger, applying blurring based on verified matches, also utilizing spatiotemporal verification. This module is managed by the SecureSphere DTMS for access control. A Government-Recognized Trusted Authority authenticates the identities stored on the Decentralized Privacy Ledger.

Key Interactions:

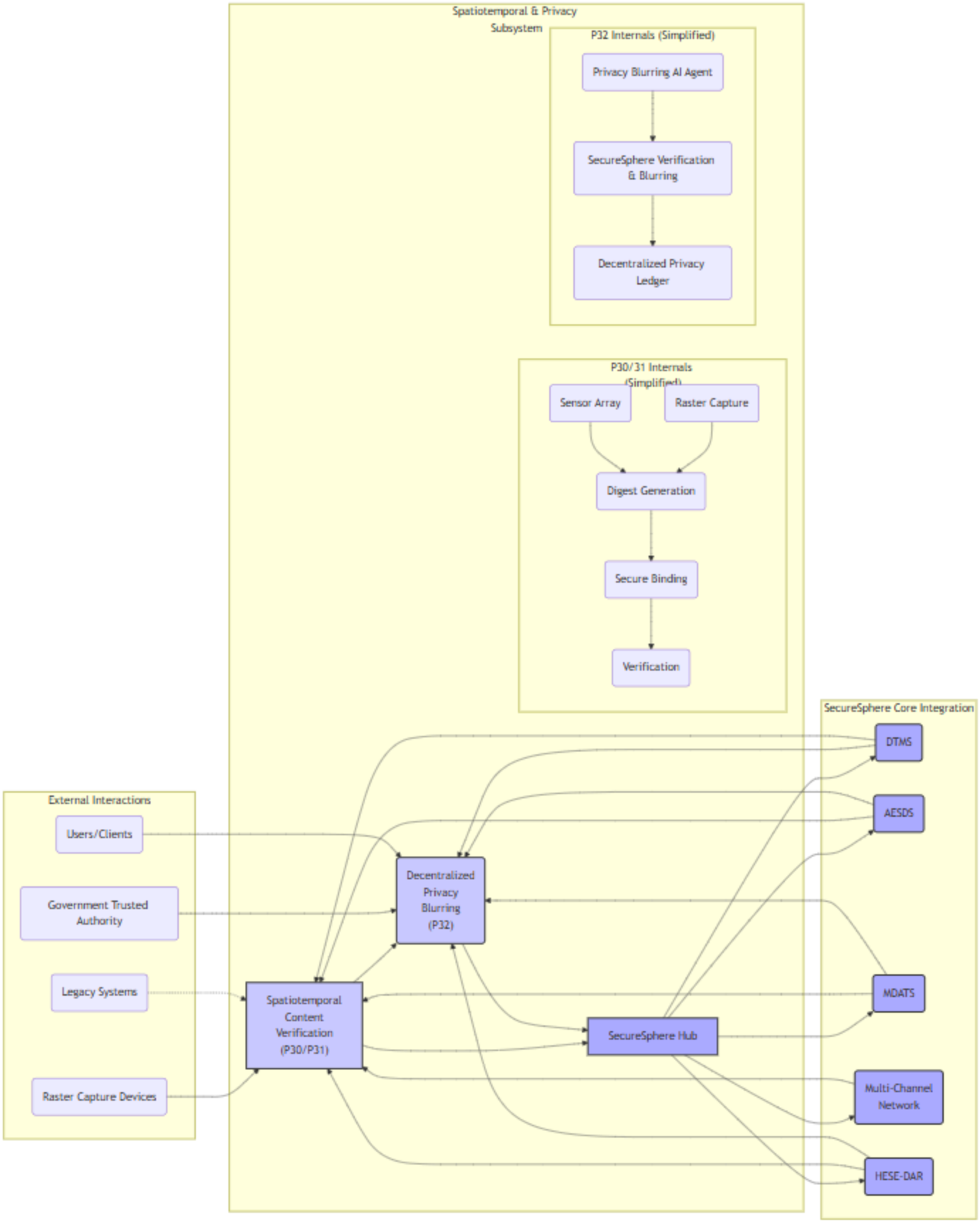
- The Spatiotemporal Digest Verification (Patent 30) feeds into the SecureSphere Spatiotemporal Verification Module (Patent 31) for content authenticity.
- The SecureSphere Spatiotemporal Verification Module (Patent 31) provides an additional layer of security to the Privacy Verification & Blurring Module (Patent 32).
- The Decentralized Privacy Blurring system (Patent 32) leverages the SecureSphere architecture (DTMS, HESE-DAR, MCN, MDATS) for secure processing, access control, and auditing. The Government-Recognized Trusted Authority verifies user identities.

This integrated diagram illustrates how these three patents synergistically enhance the security and privacy of raster content within SecureSphere, providing a comprehensive and robust solution for managing sensitive data. It also showcases the interaction and integration between each patent, and how these work together to implement a system that is both secure and privacy-preserving.

Diagram 2:

```
graph LR
    subgraph "Spatiotemporal & Privacy Subsystem"
        A["Spatiotemporal<br>Content<br>Verification<br>(P30/P31)"] --> B("Decentralized<br>Privacy<br>Blurring<br>(P32)");
        A --> C(SecureSphere Hub);
        B --> C;
        style A fill:#ccf,stroke:#333,stroke-width:2px
        style B fill:#ccf,stroke:#333,stroke-width:2px
        class A,B secure

        subgraph "P30/31 Internals (Simplified)"
            A1(Sensor Array) --> A2(Digest Generation);
            A3(Raster Capture) --> A2;
            A2 --> A4(Secure Binding);
            A4 --> A5(Verification);
        end

        subgraph "P32 Internals (Simplified)"
            B1(Privacy Blurring AI Agent) --> B2(SecureSphere Verification & Blurring);
            B2 --> B3(Decentralized Privacy Ledger);
```

```
    end
end


subgraph "SecureSphere Core Integration"
    C[SecureSphere Hub] --> D(DTMS);
    C --> E(AESDS);
    C --> F(MDATS);
    C --> G(Multi-Channel<br>Network);
    C --> H(HESE-DAR);
    D --> B;
    D --> A;
    E --> A;
    E --> B;
    F --> A;
    F --> B;
    G --> A;
    H --> A;
    H --> B;
    style C fill:#aaf,stroke:#333,stroke-width:2px
    style D fill:#aaf,stroke:#333,stroke-width:2px
    style E fill:#aaf,stroke:#333,stroke-width:2px
    style F fill:#aaf,stroke:#333,stroke-width:2px
    style G fill:#aaf,stroke:#333,stroke-width:2px
    style H fill:#aaf,stroke:#333,stroke-width:2px
    class C,D,E,F,G,H core
end

subgraph "External Interactions"
    I(Raster Capture Devices) --> A;
    J(Legacy Systems) -.-> A;
    K(Government Trusted Authority) --> B;
    L(Users/Clients) --> B;
end


linkStyle default stroke:#555,stroke-width:1px

classDef secure fill:#ccf,stroke:#333,stroke-width:2px
classDef core fill:#aaf,stroke:#333,stroke-width:2px
```



Description for Diagram 2:

This diagram illustrates the integration of the Spatiotemporal and Privacy Subsystem within the SecureSphere architecture. This subsystem comprises functionalities described in Patents 30 (Spatiotemporal Digest for Raster Content Verification), 31 (SecureSphere System with Integrated Spatiotemporal Raster Content Verification), and 32 (Decentralized Privacy Blurring Standard with SecureSphere Integration). While each patent is represented by a simplified block, the diagram highlights the detailed interactions with other SecureSphere components and external entities.

1. Spatiotemporal & Privacy Subsystem:

- **Spatiotemporal Content Verification (P30/P31 - A):** This block encapsulates the functionality of generating, binding, and verifying spatiotemporal digests for raster content (images, videos, audio). It receives input from Raster Capture Devices (I) and interacts with the SecureSphere Hub (C) for management and integration with core SecureSphere services. It also interacts with Legacy Systems (J) via appropriate adaptation mechanisms. Internally, it performs sensor data acquisition, digest generation, secure binding to the content, and verification processes.
- **Decentralized Privacy Blurring (P32 - B):** This block represents the functionality of blurring individuals' likenesses in raster content based on their privacy preferences recorded on a decentralized ledger. It receives input from users (L) regarding their privacy settings and interacts with a Government Trusted Authority (K) for identity verification. It relies heavily on the SecureSphere Hub (C) and DTMS (D) for secure operation and policy enforcement. Internally, it utilizes a Privacy Blurring AI Agent and interacts with the Decentralized Privacy Ledger.
- **Interaction (A --> B):** The Spatiotemporal Content Verification module provides context to the Decentralized Privacy Blurring module. This context, including the location and time of content capture, helps determine the appropriate level of blurring and prevents unnecessary or excessive blurring based on verified spatiotemporal data.

2. SecureSphere Core Integration:

- **SecureSphere Hub (C):** The central orchestrator and management point for the entire subsystem. It controls policy distribution, resource allocation, and communication between modules.
- **DTMS (D):** Manages trust relationships and access control for the entire subsystem, including the HESE-DAR, decentralized ledger, and other components. It enforces privacy policies and ensures that only authorized entities can access sensitive data.
- **AESDS (E):** Responsible for secure software updates and patches for all modules within the subsystem, ensuring its continued secure operation and adaptation to evolving threats.
- **MDATS (F):** Provides comprehensive audit trails for all operations within the subsystem, logging events related to spatiotemporal digest generation, verification, privacy blurring, and access control decisions. This ensures transparency and accountability.
- **Multi-Channel Network (G):** Securely transmits data between various components, including the spatiotemporal sensors, raster capture devices, HESE-DAR, and external entities.
- **HESE-DAR (H):** Provides a secure enclave for processing sensitive data, such as biometric templates used for privacy blurring and the spatiotemporal digests themselves.

3. External Interactions:

- **Raster Capture Devices (I):** Provide the input raster content (images, videos, audio) and associated spatiotemporal data to the Spatiotemporal Content Verification module.

- **Legacy Systems (J):** Integration with legacy systems is facilitated through appropriate adaptation layers, allowing the subsystem to handle content from older devices that may not provide spatiotemporal data.
- **Government Trusted Authority (K):** Provides identity verification and validation services for the Decentralized Privacy Blurring module, ensuring that privacy preferences are associated with legitimate users.
- **Users/Clients (L):** Interact with the system to set their privacy preferences, which are then recorded on the Decentralized Privacy Ledger.

This architecture demonstrates a robust and integrated approach to securing and managing raster content within the SecureSphere system. The diagram highlights the key functionalities of each patent (P30, P31, P32) and their interactions with SecureSphere's core components. The inclusion of external interactions illustrates the practical application of the subsystem in real-world scenarios.

Patent 30: Spatiotemporal Digest for Raster Content Verification

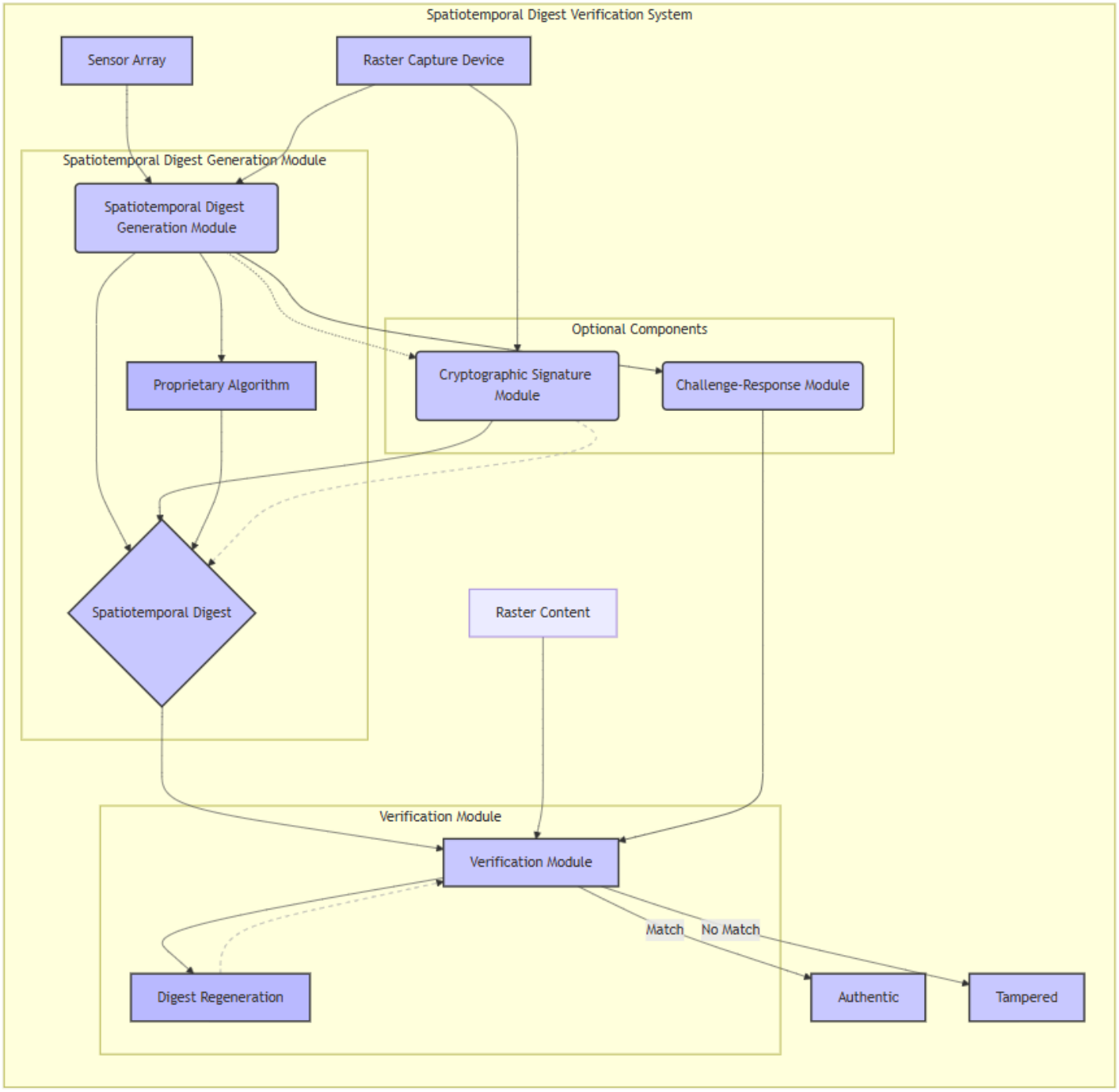
Abstract:

This patent discloses a novel system and method for verifying the authenticity and integrity of raster content (audio, images, video) by generating a spatiotemporal digest representing the physical reality captured by the raster data. This spatiotemporal metadata digest is derived from detailed sensor measurements of the physical environment, including spatial, temporal, and other relevant physical parameters. The digest, generated through a presently undisclosed process based on private theoretical and experimental research, exhibits provable non-isomorphism with the raster content itself. This system provides a one-way verification link between the raster content and the physical reality it represents. The system further incorporates traditional cryptographic signature verification for additional security and legal verifiability, operating independently of the spatiotemporal digest. This dual-layered approach provides robust protection against content manipulation and forgery.

Diagram:

```
graph LR
    subgraph "Spatiotemporal Digest Verification System"
        A[Sensor Array] --> B(Spatiotemporal Digest Generation Module);
        C[Raster Capture Device] --> B;
        B --> D{Spatiotemporal Digest};
        D --> E[Verification Module];
        F[Raster Content] --> E;
        E -- Match --> G[Authentic]
        E -- No Match --> H[Tampered]
        B -.-> I(Cryptographic Signature Module);
        C --> I;
        I --> D;
        style I fill:#ccf,stroke:#333,stroke-width:2px
        class I optional

        subgraph "Spatiotemporal Digest Generation Module"
            B --> J[Proprietary Algorithm];
            J --> D;
            style J fill:#bbf,stroke:#333,stroke-width:2px
        end

        subgraph Verification Module
            E --> K[Digest Regeneration];
            K --> E;
            style K fill:#bbf,stroke:#333,stroke-width:2px
        end

        subgraph Optional Components
            I --> D;
            B --> L(Challenge-Response Module);
```

```
        L --> E;
        style L fill:#ccf,stroke:#333,stroke-width:2px
    end

    style A fill:#ccf,stroke:#333,stroke-width:2px
    style B fill:#ccf,stroke:#333,stroke-width:2px
    style C fill:#ccf,stroke:#333,stroke-width:2px
    style D fill:#ccf,stroke:#333,stroke-width:2px
    style E fill:#ccf,stroke:#333,stroke-width:2px
    style G fill:#ccf,stroke:#333,stroke-width:2px
    style H fill:#ccf,stroke:#333,stroke-width:2px


    class A,B,C,D,E,G,H secure
    class J,K,L module

end


classDef secure fill:#ccf,stroke:#333,stroke-width:2px
classDef module fill:#bbf,stroke:#333,stroke-width:2px
linkStyle 0,1,2,3,4,5,6,7,8,9,10,11,12 stroke:#555,stroke-width:1px
linkStyle 13,14 stroke:#aaa,stroke-width:1px,stroke-dasharray: 5 5
```



Description of Diagram:

The accompanying diagram illustrates the architecture of the Spatiotemporal Digest for Raster Content Verification system (Patent 30). The system comprises a sensor array, a raster capture device, and a verification module, working in conjunction with a proprietary spatiotemporal digest generation algorithm. Optional components include a cryptographic signature module and a challenge-response module, enhancing security and verification efficiency.

1. Spatiotemporal Data Acquisition and Digest Generation:

- **Sensor Array (A):** This array captures multi-parameter spatiotemporal data representing the physical environment surrounding the raster content capture. This data includes, but is not limited to, spatial

coordinates, temporal information, temperature, pressure, electromagnetic fields, gravitational fields, acoustic waves, and particle density. The specific parameters and sampling rate are configurable based on the application requirements.

- **Raster Capture Device (C):** This device captures the raster content (audio, images, video) from the physical environment. This device may be integrated with the sensor array (A) to ensure precise synchronization of spatiotemporal data and raster content acquisition.

- **Spatiotemporal Digest Generation Module (B):** This module processes the spatiotemporal data acquired by the sensor array (A), utilizing a proprietary algorithm (J) to generate a unique spatiotemporal digest (D). This algorithm is based on private research and exhibits a provable lack of isomorphism between the input spatiotemporal data and the resulting digest, ensuring its non-invertibility and resistance to forgery. The detailed workings of this algorithm are considered proprietary information.

- **Proprietary Algorithm (J):** This module houses the core intellectual property, a proprietary algorithm for generating the spatiotemporal digest. This algorithm leverages principles of non-isomorphism, ensuring that the digest cannot be easily reverse-engineered to reconstruct the original spatiotemporal data. The exact implementation details are undisclosed for proprietary reasons.

2. Verification and Authentication:

- **Spatiotemporal Digest (D):** This is the output of the Spatiotemporal Digest Generation Module (B). It represents a unique, cryptographically secure fingerprint of the physical environment at the time of raster content capture.

- **Verification Module (E):** This module is responsible for verifying the authenticity of the raster content. It receives as input both the raster content (F) and a purported spatiotemporal digest. To perform verification, it regenerates the digest using the associated spatiotemporal data (via the Digest Regeneration module, K). A comparison between the provided digest and the regenerated digest determines the authenticity of the raster content. A match indicates authenticity (G), while a mismatch signifies tampering (H).

- **Digest Regeneration (K):** This sub-module within the Verification Module (E) recreates the spatiotemporal digest based on the spatiotemporal data associated with the received raster content. This is crucial for the comparison process.

3. Optional Security Enhancements:

- **Cryptographic Signature Module (I):** This module (optional) generates and verifies digital signatures for the raster content using standard cryptographic techniques. This signature acts as a secondary layer of verification and provides independent legal verifiability of the raster content. The cryptographic signature is linked to the spatiotemporal digest (D) to improve the verification process.

- **Challenge-Response Module (L):** This module (optional) is designed for quick verification. It generates a challenge-response token based on a cryptographic hash of a subset of the spatiotemporal data, allowing for efficient verification without transmitting the entire spatiotemporal data set.

The system is designed to ensure the integrity and authenticity of the raster content by linking it to a unique spatiotemporal representation of its capture environment, protected by non-isomorphism, cryptography, and optional redundancy.

Claims:

1. A system for verifying the authenticity and integrity of raster content, comprising:

    - a sensor array configured to capture spatiotemporal data representing a physical environment;
    - a digest generation module configured to process said spatiotemporal data and generate a spatiotemporal digest, wherein said digest exhibits provable non-isomorphism with any raster content derived from the captured physical environment;
    - a raster capture device configured to capture raster content of the physical environment; and
    - a verification module configured to compare a spatiotemporal digest with a claimed association to said raster content, wherein a match indicates authenticity of said raster content.

2. The system of claim 1, wherein the sensor array captures data related to at least three of the following physical parameters: spatial coordinates, time, temperature, pressure, electromagnetic fields, gravitational fields, acoustic waves, and particle density.

3. The system of claim 1, wherein the digest generation module utilizes a proprietary algorithm based on private theoretical and experimental research, demonstrating a provable lack of isomorphism between the spatiotemporal data and the generated digest.

4. The system of claim 1, further comprising a cryptographic signature module configured to generate and verify digital signatures for said raster content, wherein said digital signatures operate independently of the spatiotemporal digest.

5. A method for verifying the authenticity and integrity of raster content, comprising the steps of:

    - capturing spatiotemporal data of a physical environment using a sensor array;
    - generating a spatiotemporal digest from said spatiotemporal data using a digest generation module;
    - capturing raster content of the physical environment using a raster capture device;
    - associating the spatiotemporal digest with said raster content; and
    - verifying the authenticity of said raster content by comparing the associated spatiotemporal digest with a provided spatiotemporal digest.

6. The method of claim 5, further comprising the steps of:

    - generating a digital signature for the raster content using a cryptographic signature module; and
    - verifying the digital signature of the raster content.

7. The system of claim 1, wherein the provable non-isomorphism ensures that the spatiotemporal digest cannot be used to reconstruct the original spatiotemporal data or any raster content derived therefrom.

8. The method of claim 5, wherein the spatiotemporal digest is generated using a quantum-resistant hashing algorithm.

9. The system of claim 4, wherein the cryptographic signature module utilizes post-quantum cryptography (PQC).

10. The system of claim 1, wherein the raster content includes at least one of the following: audio recordings, images, and video recordings.

11. The system of claim 1, wherein the verification module is located within a hardware-enforced secure encrypted enclave (HESE-DAR), thereby protecting the verification process from unauthorized access and tampering.

12. The system of claim 1, wherein the sensor array is integrated into a raster capture device, thereby synchronizing the capture of spatiotemporal data and raster content.

13. The system of claim 1, wherein the spatiotemporal digest is encrypted using a post-quantum cryptography (PQC) algorithm, enhancing security against future cryptographic threats.

14. The system of claim 1, wherein the spatiotemporal digest is stored within a tamper-evident storage medium, further improving the system's integrity.

15. The system of claim 1, further comprising a module for generating a challenge-response using a hash of selected segments of the spatiotemporal data for quick verification without transmitting full spatiotemporal data.

16. A method according to claim 5, wherein said association of spatiotemporal digest and raster content includes metadata generated by the sensor array, timestamping said association with precise temporal information.

Patent 31: SecureSphere System with Integrated Spatiotemporal Raster Content Verification

Abstract:

This invention enhances secure computing architectures like SecureSphere with a novel spatiotemporal content verification module. Located within a HESE-DAR enclave and controlled by the DTMS, this module generates unique, non-invertible spatiotemporal digests ("spatiotemporal metadata digests") from sensor data captured synchronously with raster content. These digests are cryptographically bound to the content, creating an immutable link to its physical origin. Verification occurs within the HESE-DAR, comparing received digests against regenerated ones, with digital signatures providing a secondary layer of security. Quick verification and legacy system compatibility enhance practicality. This integration significantly improves content authenticity and integrity validation.

These revised claims are narrower, focusing specifically on the novel SecureSphere module and its components, detailing the integration with HESE-DAR and DTMS. The claims emphasize the non-invertibility and non-isomorphism of the spatiotemporal digest, which are key aspects of the innovation. They also incorporate the quick verification and legacy system compatibility features for added practicality. This approach strikes a balance between novelty and breadth, offering robust protection for the core invention while providing specific implementation details within the SecureSphere context.

Field of the Invention: This invention pertains to secure computing architectures and specifically to verifying the authenticity and integrity of raster content (audio, images, video) integrated into such a system using spatiotemporal data binding.

Background of the Invention:

Existing secure computing architectures, while offering robust protection against various software and hardware attacks, lack a mechanism to irrefutably link ingested raster content to the physical reality it represents. Traditional methods relying on cryptographic hashes or digital signatures applied to the raster data itself fail to address potential manipulation of the original capture environment or subsequent metadata alteration. This necessitates a novel approach to verify the provenance and integrity of raster content within a secure computing architecture.

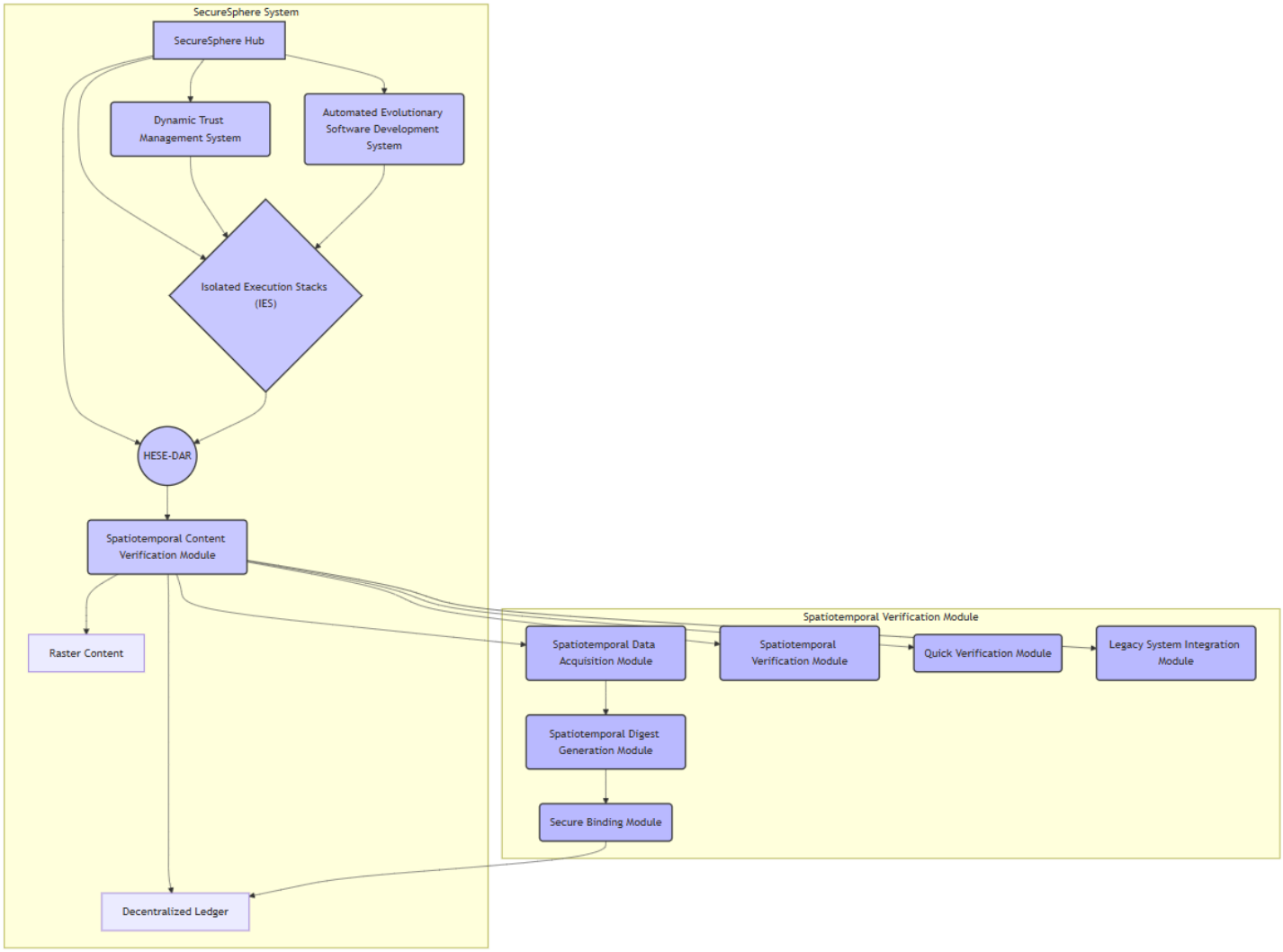
Summary of the Invention:

This invention discloses a novel system and method within a secure computing architecture, such as SecureSphere, integrating spatiotemporal data binding for comprehensive raster content verification. A dedicated SecureSphere module, operating within a Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) under the control of the Dynamic Trust Management System (DTMS), generates a unique, non-invertible spatiotemporal digest ("spatiotemporal metadata digest") derived from sensor data captured concurrently with the raster content. This digest, provably non-isomorphic to the raster data and its associated metadata, is inextricably linked to the content within the secure architecture. This architecture not only verifies content integrity but also cryptographically binds it to its spatiotemporal origin, providing robust protection against sophisticated manipulation and forgery. Quick verification and legacy system compatibility enhance practicality.

Diagram:

```
graph
    subgraph SecureSphere System
        A[SecureSphere Hub] --> B(Dynamic Trust Management System);
        A --> C(Automated Evolutionary Software Development System);
        A --> D{"Isolated Execution Stacks (IES)"};
        A --> E((HESE-DAR));
        B --> D;
        C --> D;
        D --> E;
        E --> F(Spatiotemporal Content Verification Module);
        F --> G[Decentralized Ledger];
        F --> H[Raster Content];

        style A fill:#ccf,stroke:#333,stroke-width:2px
        style B fill:#ccf,stroke:#333,stroke-width:2px
        style C fill:#ccf,stroke:#333,stroke-width:2px
        style D fill:#ccf,stroke:#333,stroke-width:2px
        style E fill:#ccf,stroke:#333,stroke-width:2px
        style F fill:#ccf,stroke:#333,stroke-width:2px

        class A,B,C,D,E,F secure

    end

    subgraph "Spatiotemporal Verification Module"
        F --> I(Spatiotemporal Data Acquisition Module);
        I --> J(Spatiotemporal Digest Generation Module);
        J --> K(Secure Binding Module);
        K --> G;
        F --> L(Spatiotemporal Verification Module);
        F --> M(Quick Verification Module);
        F --> N(Legacy System Integration Module);

        style I fill:#bbf,stroke:#333,stroke-width:2px
        style J fill:#bbf,stroke:#333,stroke-width:2px
        style K fill:#bbf,stroke:#333,stroke-width:2px
        style L fill:#bbf,stroke:#333,stroke-width:2px
```

```
    style M fill:#bbf,stroke:#333,stroke-width:2px
    style N fill:#bbf,stroke:#333,stroke-width:2px

    class I,J,K,L,M,N module

end


classDef secure fill:#ccf,stroke:#333,stroke-width:2px
classDef module fill:#bbf,stroke:#333,stroke-width:2px


linkStyle 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 stroke:#555,stroke-width:1px
```



Description of Diagram:

The accompanying diagram illustrates the architecture of a secure computing system enhanced with integrated spatiotemporal raster content verification. The system comprises existing SecureSphere components and a novel Spatiotemporal Content Verification Module.

1. SecureSphere Core Components:

- **SecureSphere Hub (A):** Orchestrates and manages all system components, including the Dynamic Trust Management System (DTMS), the Automated Evolutionary Software Development System (AESDS), Isolated Execution Stacks (IES), and the Hardware-Enforced Secure Encrypted Enclave (HESE-DAR).

- **Dynamic Trust Management System (DTMS) (B):** Manages trust relationships and access control across SecureSphere components, including the HESE-DAR and the Spatiotemporal Content Verification Module.

- **Automated Evolutionary Software Development System (AESDS) (C):** Provides continuous software monitoring, updates, and security patching for all SecureSphere components.

- **Isolated Execution Stacks (IES) (D):** Provide hardware-enforced isolation for applications and processes, ensuring secure execution environments.

- **Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) (E):** A hardware-protected enclave for secure storage and processing of sensitive data and the Spatiotemporal Content Verification Module.

2. Spatiotemporal Content Verification Module (F):

This module, residing within the HESE-DAR under DTMS control, comprises the following sub-modules:

- **Spatiotemporal Data Acquisition Module (SDAM) (I):** Captures multi-parameter spatiotemporal data from the physical environment concurrent with raster content acquisition.

- **Spatiotemporal Digest Generation Module (SDGM) (J):** Processes the spatiotemporal data from the SDAM, utilizing a proprietary non-invertible algorithm, generating a unique spatiotemporal digest ("spatiotemporal metadata digest") exhibiting provable non-isomorphism with the raster content.

- **Secure Binding Module (SBM) (K):** Cryptographically binds the spatiotemporal digest generated by the SDGM to the raster content within the HESE-DAR. This binding is recorded on the SecureSphere Decentralized Ledger.

- **Spatiotemporal Verification Module (SVM) (L):** Compares a received spatiotemporal digest with a regenerated digest from associated spatiotemporal data within the HESE-DAR, confirming authenticity.

- **Quick Verification Module (QVM) (M):** Performs rapid verification using a challenge-response mechanism, based on a hash of select spatiotemporal data segments, without requiring full data transmission.

- **Legacy System Integration Module (LSIM) (N):** Facilitates integration with legacy systems lacking spatiotemporal data acquisition capabilities, utilizing established cryptographic methods as a fallback verification mechanism.

3. Data Flow and System Interactions:

The SDAM acquires spatiotemporal data, which is processed by the SDGM within the HESE-DAR to generate a spatiotemporal digest. The SBM securely binds this digest to the raster content. The SVM performs verification, comparing received digests with those regenerated from associated data within the HESE-DAR. The QVM provides a fast verification path, while the LSIM facilitates legacy system compatibility. The DTMS controls access to all modules within the HESE-DAR. All significant events are recorded on the Decentralized Ledger, ensuring auditability and transparency.

This architecture integrates a novel spatiotemporal verification system into the existing SecureSphere framework, providing a robust and verifiable method for linking raster content to its physical origin, thus enhancing the overall security and trustworthiness of the system.

Detailed Description:

This invention enhances the SecureSphere architecture with the following integrated components:

1. **Spatiotemporal Data Acquisition Module (SDAM):** Comprising a sensor array integrated with or synchronized with the raster capture device, the SDAM acquires multi-parameter spatiotemporal data (spatial coordinates, time, temperature, pressure, electromagnetic fields, gravitational fields, acoustic waves, particle density, etc.) representing the physical environment during raster content capture. This data is securely transmitted to the HESE-DAR via dedicated, authenticated SecureSphere channels (P3).

2. **Spatiotemporal Digest Generation Module (SDGM) (within HESE-DAR):** Utilizing a proprietary, non-invertible algorithm based on private research, the SDGM processes the received spatiotemporal data and generates a unique spatiotemporal digest ("spatiotemporal metadata digest"). This digest is provably non-isomorphic to the raster content and its associated metadata, ensuring it cannot be reconstructed from the raster data alone.

3. **Secure Binding Module (SBM) (within HESE-DAR):** The SBM cryptographically binds the spatiotemporal digest to the acquired raster content within the HESE-DAR, creating an immutable link between the content and its spatiotemporal origin. This binding is recorded on the SecureSphere Decentralized Ledger (P13, P15) under DTMS control, ensuring tamper-evident provenance tracking.

4. **Spatiotemporal Verification Module (SVM) (within HESE-DAR):** Upon receiving a verification request, the SVM, operating within the HESE-DAR, regenerates the spatiotemporal digest from the associated data and compares it with the stored, bound digest. A match confirms content authenticity and integrity. Cryptographic signature verification (P24) provides an independent, secondary authentication layer.

5. **Quick Verification Module (QVM) (within HESE-DAR):** The QVM employs a challenge-response mechanism based on a hash of select portions of the spatiotemporal data, enabling rapid verification without full data transmission.

6. **Legacy System Integration Module (LSIM):** The LSIM, leveraging the Isomorphic Architecture Monitoring and Adaptation (IAMA) module (P16), enables secure integration with legacy systems lacking spatiotemporal data acquisition capabilities, utilizing cryptographic verification (PQC - P5) as a fallback mechanism.

Claims:

Independent Claim 1:

A secure computing architecture, such as SecureSphere, comprising a Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) and a Dynamic Trust Management System (DTMS), characterized by a Spatiotemporal Content Verification Module located within said HESE-DAR, said module comprising:

a) a Spatiotemporal Data Acquisition Module (SDAM) configured to capture multi-parameter spatiotemporal data from a physical environment; b) a Spatiotemporal Digest Generation Module (SDGM) configured to generate a unique, non-invertible spatiotemporal digest from said spatiotemporal data, wherein said digest exhibits provable non-isomorphism with raster content captured from said environment; c) a Secure Binding Module (SBM) configured to cryptographically bind said spatiotemporal digest to said raster content within the HESE-DAR under DTMS control; and d) a Spatiotemporal Verification Module (SVM) configured to verify the authenticity and integrity of said raster content by comparing a received spatiotemporal digest against a regenerated digest from the associated data, said verification occurring within the HESE-DAR.

Dependent Claims:

2. The architecture of claim 1, wherein the SDAM synchronizes the capture of spatiotemporal data with the raster content acquisition process.

3. The architecture of claim 1, wherein the SDGM utilizes a proprietary algorithm based on private research, demonstrating provable non-isomorphism between the spatiotemporal data and the generated digest.

4. The architecture of claim 1, wherein the SBM records the binding of the spatiotemporal digest and the raster content on a Decentralized Ledger under DTMS control.

5. The architecture of claim 1, further comprising a Quick Verification Module (QVM) that employs a challenge-response mechanism based on a hash of select portions of the spatiotemporal data for efficient verification.

6. The architecture of claim 1, further comprising a Legacy System Integration Module (LSIM) that leverages an Isomorphic Architecture Monitoring and Adaptation (IAMA) module to enable secure integration with legacy systems and employs cryptographic methods as a fallback verification mechanism.

7. The architecture of claim 1, wherein said HESE-DAR and said DTMS are components of a SecureSphere secure computing system.

Patent 32: Decentralized Privacy Blurring Standard with SecureSphere Integration

This innovation proposes a society-wide standard for the "right to be private in public," leveraging blockchain technology, AI, and SecureSphere for automated privacy blurring in raster content (images and video). Individuals can opt into a privacy protection program by registering their biometric data (faces) on a decentralized, permissioned blockchain ledger managed under SecureSphere's Dynamic Trust Management System (DTMS).

System Architecture:

Privacy Ledger (managed by SecureSphere DTMS): A permissioned blockchain ledger records individuals who have opted into the privacy protection program. This includes securely stored and anonymized biometric templates (faces), potentially using homomorphic encryption, linked to a unique identifier. SecureSphere's

Decentralized Governance mechanisms are used to allow verified changes and edits and govern this system's functions and operational modes of use and access control and enforcement parameters.

Privacy Blurring AI Agent: Residing on raster capture devices (smartphones, professional cameras), this AI agent uses a combination of AI models. First, it identifies human faces in raster content. This then runs through SecureSphere-validated processes. This agent attempts to match a identified subject against the anonymized templates securely and transparently fetched from the Privacy Ledger (by SecureSphere-authorized means). Matches are automatically reported via authenticated communication using SecureSphere technologies (possibly Quantum-Resistant communication for increased trust, or a high integrity mechanism) to the secure central component for further checks and processing and potential metadata association linking and confirmation.

SecureSphere Verification & Blurring Module (in HESE-DAR): SecureSphere has an additional module to check face matches to protect against manipulation and adversarial attacks. This operates within the HESE-DAR (P24), secured by DTMS (P4). Using authenticated and trusted queries that conform to DTMS policy mechanisms and trust negotiations (possibly with MPC, referencing innovation idea #6 from prior), it receives anonymized identifiers and confirmation reports for verified faces from multiple devices, performs cross-checks to handle false-positive and other system limitations or challenges, and can handle partial obscuring requests based on verified matches and related security parameters based on metadata context during matching and other privacy parameters as required. Once the matching process concludes, the metadata confirming this result will be saved back onto the ledger through verifiable secure pathways (SecureSphere processes again).

Blurring Mechanism (in Privacy Blurring Agent): Based on verified confirmation reports received, the identified subject’s likeness is automatically blurred within the raster content (by privacy policies). This could entail blurring just a portion of a frame based on the context provided from a human interaction request via a private and authenticated communications channel; an option to implement for greater context and operational freedom that will make the use more practically viable and widely adoptable and accepted in legal practice across many professional usages such as surveillance and enforcement processes and legal proceedings. Further aspects can be handled by this process in more sophisticated implementations using the IAMA technology described in our existing SecureSphere designs.
Let's brainstorm extensions to the Decentralized Privacy Blurring system, focusing on authentication, access control, and integration with trusted government networks. We'll also refine the claims.

Brainstorming Extensions:

1. **Government-Verified Identity:** Integrate with existing or planned government-verified digital identity systems. Individuals could register for privacy protection via a secure, government-vetted process, ensuring the integrity of the Privacy Ledger.

2. **Tiered Privacy Levels:** Allow users to define different levels of blurring (e.g., partial face blurring, full anonymization) based on context or sensitivity. This might involve adding context metadata to the privacy setting itself, dynamically changing its functionality.

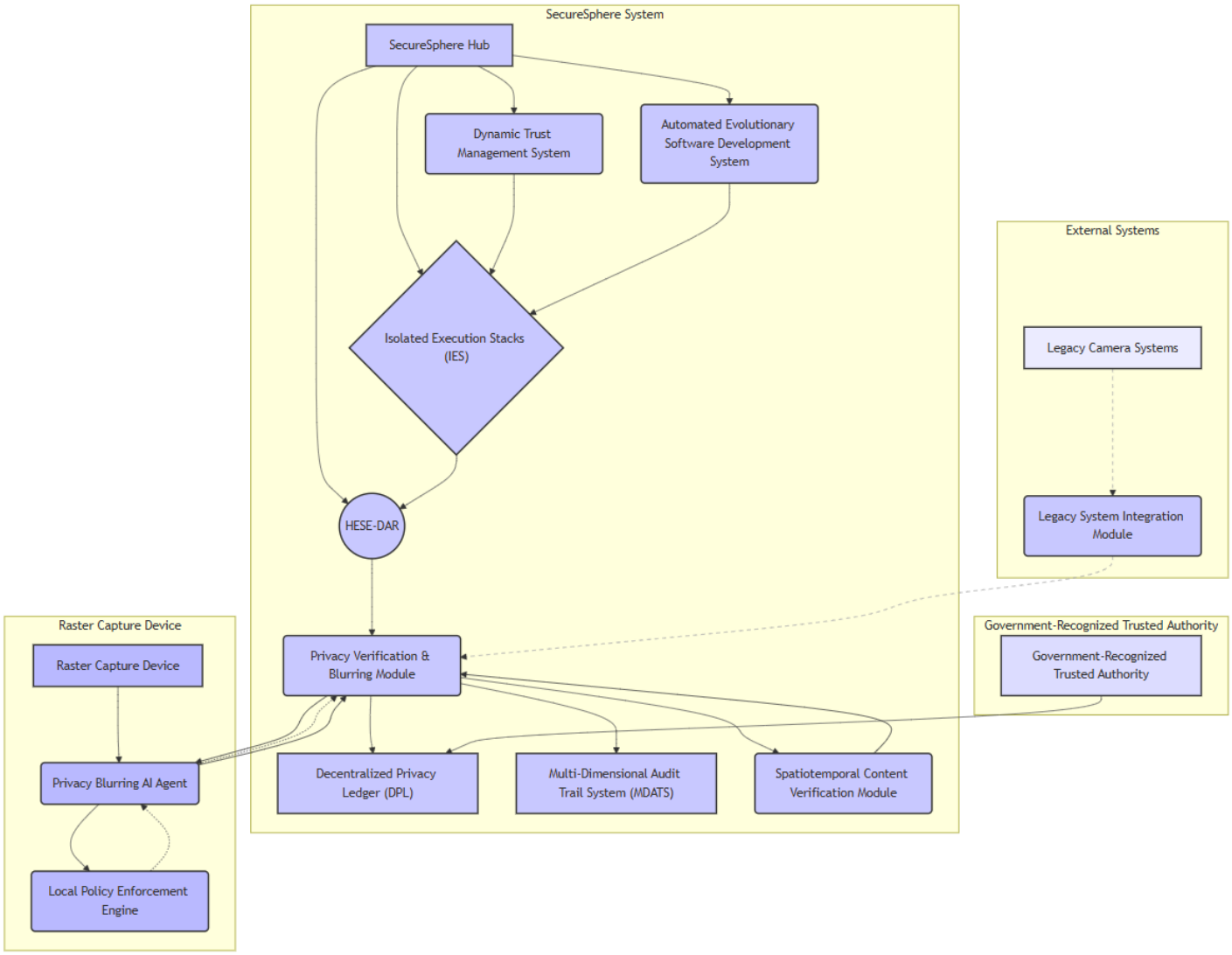
3. **Trusted Network Integration:** Integrate with government-managed trusted networks for secure communication between the Privacy Blurring AI Agent and the SecureSphere Verification & Blurring Module, establishing end-to-end encrypted and trusted high-integrity communication between devices. This will utilize the authentication protocols established and defined for these trusted channels, ensuring trust and integrity during communication between systems.

4. **Data Minimization:** Develop mechanisms within the system for securely handling minimized biometric data. The actual biometric information will only exist minimally in memory; SecureSphere will provide its trusted management system through its internal components.

5. **Transparency and Auditability:** Enhanced logging and reporting features for both system administrators and users. This enhances the systems trustworthiness and transparency. Use of both digital and physical audit trails (from MDATS (P17) from our existing designs) to provide additional security and increase trust in the integrity and security and verifiable function of this system.

Diagram:

```
graph
    subgraph SecureSphere System
        A[SecureSphere Hub] --> B(Dynamic Trust Management System);
        A --> C(Automated Evolutionary Software Development System);
        A --> D{"Isolated Execution Stacks (IES)"};
        A --> E((HESE-DAR));
        B --> D;
        C --> D;
        D --> E;
        E --> F(Privacy Verification & Blurring Module);
        F --> G["Decentralized Privacy Ledger (DPL)"];
        F --> H["Multi-Dimensional Audit Trail System (MDATS)"];
        F --> I(Spatiotemporal Content Verification Module);
        style A fill:#ccf,stroke:#333,stroke-width:2px
        style B fill:#ccf,stroke:#333,stroke-width:2px
        style C fill:#ccf,stroke:#333,stroke-width:2px
        style D fill:#ccf,stroke:#333,stroke-width:2px
        style E fill:#ccf,stroke:#333,stroke-width:2px
        style F fill:#ccf,stroke:#333,stroke-width:2px
        style G fill:#ccf,stroke:#333,stroke-width:2px
        style H fill:#ccf,stroke:#333,stroke-width:2px
        style I fill:#ccf,stroke:#333,stroke-width:2px
        class A,B,C,D,E,F,G,H,I secure
    end

    subgraph Raster Capture Device
        J[Raster Capture Device] --> K(Privacy Blurring AI Agent);
        K --> L(Local Policy Enforcement Engine);
        K -.-> F;
        L -.-> K;
        style J fill:#bbf,stroke:#333,stroke-width:2px
        style K fill:#bbf,stroke:#333,stroke-width:2px
        style L fill:#bbf,stroke:#333,stroke-width:2px
        class J,K,L device
    end

    subgraph "Government#8209;Recognized Trusted Authority"
        M[Government-Recognized Trusted Authority] --> G;
        style M fill:#ddf,stroke:#333,stroke-width:2px
        class M authority
    end

    subgraph External Systems
    N[Legacy Camera Systems] --> O(Legacy System Integration Module);
    O --> F;
    style N fill:#eef,stroke:#333,stroke-width:2px
    style O fill:#ccf,stroke:#333,stroke-width:2px
    class N,O external
    end

    linkStyle 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 stroke:#555,stroke-width:1px
    linkStyle 16,17 stroke:#aaa,stroke-width:1px,stroke-dasharray: 5 5

    K --> F;
    F --> K;
    I --> F;


    classDef secure fill:#ccf,stroke:#333,stroke-width:2px
    classDef device fill:#bbf,stroke:#333,stroke-width:2px
    classDef authority fill:#ddf,stroke:#333,stroke-width:2px
    classDef external fill:#eef,stroke:#333,stroke-width:2px
```



Detailed Description of the Diagram:

This diagram illustrates the architecture of a decentralized privacy-preserving raster content processing system integrated with SecureSphere. The system is composed of three main subsystems: the SecureSphere infrastructure, the raster capture device, and a Government-Recognized Trusted Authority. Data flows are represented by arrows, with dashed lines indicating optional or conditional pathways.

1. SecureSphere Infrastructure:

SecureSphere Hub (A): Orchestrates and manages all SecureSphere components.

Dynamic Trust Management System (DTMS) (B): Manages access control and trust relationships within SecureSphere.

Automated Evolutionary Software Development System (AESDS) (C): Manages software updates and security patching.

Isolated Execution Stacks (IES) (D): Provide hardware-enforced isolation for applications and processes.

Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) (E): Provides a secure environment for sensitive data processing. This includes the Secure Key Management (J) for the entire system.

Privacy Verification & Blurring Module (F): A SecureSphere module (within the HESE-DAR) responsible for verifying identity matches and issuing blurring directives.

Decentralized Privacy Ledger (DPL) (G): A permissioned blockchain ledger, managed by the DTMS, storing anonymized biometric templates linked to verified identities and access tokens.

Multi-Dimensional Audit Trail System (MDATS) (H): Records all system actions for auditing and accountability.

Spatiotemporal Content Verification Module (I) (Patent 31): Verifies the authenticity and integrity of the captured raster content through spatiotemporal data analysis. This aids in preventing manipulation of the context surrounding a capture.

2. Raster Capture Device: This subsystem comprises components residing on the image capture device:

Raster Capture Device (K): The device capturing the raster content (e.g., smartphone, professional camera).

Privacy Blurring AI Agent (PBAA) (L): A software agent within the device responsible for face detection, anonymized biometric hashing (N,O), and communication with the SecureSphere system.

Local Policy Enforcement Engine (LPEE) (M): Enforces real-time, context-aware privacy policies, allowing for pre-blurring operations.

3. Government-Recognized Trusted Authority:

Government-Recognized Trusted Authority (P): Authenticates user identities and verifies the integrity of biometric data added to the DPL.
4. SecureSphere Communication (Q): SecureSphere's Multi-Channel Network facilitates secure and authenticated communication between the devices and the SecureSphere system.

5. External Systems (R, S): This subsystem enables integration with legacy camera systems (R) via a Legacy System Integration Module (S) to prevent privacy leaks.

Data Flow: The PBAA (L) detects faces in the captured raster content and performs anonymized biometric hashing (O). It then transmits this hash via the MCN (Q) to the SPVBM (F) within SecureSphere's HESE-DAR (E). The LPEE (M) enforces locally defined policies. The SPVBM then compares the hash against the DPL (G), and based on verified matches from the Trusted Authority (P), issues blurring directives back to the PBAA via the MCN (Q), leveraging the spatiotemporal verification (I) to improve the integrity of the system. The entire process is logged by MDATS (H). The Legacy System Integration Module (S) helps to integrate with older camera systems that don't have all of the described capabilities, following SecureSphere's design implementations and ensuring that privacy is enhanced and improved while also ensuring wide compatibility with other hardware and systems.

This detailed description complements the diagram, providing a comprehensive understanding of the system's architecture, functionality, data flow, and interactions between its various components and subsystems. The descriptions ensure there is no confusion about the processes involved and the design characteristics that allow these to function correctly and securely.

Independent Claim 1:

A system for privacy-preserving processing of raster content within a secure computing architecture, comprising: (a) a decentralized, permissioned blockchain ledger securely storing anonymized biometric templates of individuals who have opted into a privacy protection program, their biometric templates cryptographically protected and their identities authenticated by a government-recognized trusted authority, said ledger managed by a secure computing architecture's Dynamic Trust Management System; (b) a plurality of raster capture devices, each comprising a Privacy Blurring AI Agent configured to identify human faces within captured raster content, transmit anonymized biometric hashes, securely request matching against associated data from said secure architecture through authenticated pathways within government-recognized trusted networks with confirmed policies, processes and trust relationships based on pre-negotiated consent-based security mechanisms; (c) a secure computing architecture, such as SecureSphere, comprising a Verification and Blurring Module residing within a Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) controlled by said Dynamic Trust Management System, configured to independently check match results received, process access requests based on dynamic privacy levels specified by authorized and confirmed metadata associated with identifiers on the Privacy Ledger that have verified identities linked to a biometric data representation in an appropriately secured data management format and access pattern and workflow controlled by policies implemented on the Dynamic Trust Management System (DTMS); and (d) a blurring mechanism within each Privacy Blurring AI Agent applying automatic blurring to identified subjects based on policy enforcement processes established, defined and confirmed within the secure architecture upon verification completion based on received data and validated parameters confirmed using authenticated protocols within SecureSphere, producing outputs handled according to verified processes of operation managed within the secure architecture and recorded according to policy enforcement protocols as part of secure management and auditable governance processes.

Dependent Claims:

2. The system of claim 1, wherein the anonymized biometric templates utilize homomorphic encryption for secure processing and authorized access based on policy compliance and confirmed usage situations managed by the Dynamic Trust Management System.

3. The system of claim 1, wherein the secure computing architecture is SecureSphere, utilizing SecureSphere's Multi-Channel Network (P3) and DTMS (P4) for secure communication and access control.

4. The system of claim 1, wherein the government-recognized trusted authority verifies user identities via government-issued digital identity credentials, verifying this data through authenticated pathways and SecureSphere mechanisms, ensuring this data's integrity and security according to secure policies and protocols.

5. The system of claim 1, wherein the Privacy Blurring AI Agent supports dynamic privacy levels based on metadata contexts for a privacy policy established according to the specifications managed in accordance with government policy mandates, established standards for verified operations managed by appropriate governmental entities that provide authorized and confirmed mechanisms for handling, verification and storage of related policy considerations, data processing and handling requirements.

6. The system of claim 1, wherein the secure computing architecture generates multi-dimensional audit trails (MDATS—Patent 17) for all operations related to privacy blurring, recording all information on both physical and digital audit logs to provide maximum integrity, accountability and verifiability and that further increases security.

7. The system of claim 1, wherein the system incorporates Data Minimization principles ensuring that the actual biometric data is handled securely according to established security parameters controlled according to SecureSphere's policy management procedures in the DTMS and HESE-DAR systems.

Independent Claim 1:

A system for privacy-preserving processing of raster content within a SecureSphere secure computing architecture, comprising:

(a) a Decentralized Privacy Ledger (DPL) operating within a SecureSphere zone, said DPL implemented as a permissioned blockchain ledger and managed by SecureSphere's Dynamic Trust Management System (DTMS), said DPL storing anonymized biometric templates of individuals authenticated via a government-recognized trusted authority, wherein said templates are encrypted using homomorphic encryption within a Hardware-Enforced Secure Encrypted Enclave (HESE-DAR) and linked to revocable, time-limited access tokens;

(b) a plurality of raster capture devices, each comprising: (i) a Privacy Blurring AI Agent (PBAA) configured to identify human faces within captured raster content, generate anonymized biometric hashes of said faces, and securely transmit said hashes to the SecureSphere system via SecureSphere's Multi-Channel Network (MCN) using authenticated, encrypted communication channels within government-recognized trusted networks; (ii) a Local Policy Enforcement Engine (LPEE) that implements and enforces real-time, context-aware dynamic privacy policies, allowing for on-device pre-blurring based on locally stored anonymized hashes, and transmitting metadata indicative of pre-blurring actions to the SecureSphere system;

(c) a SecureSphere Spatiotemporal Content Verification Module (SCVM) as described in Patent 31, said SCVM configured to capture and analyze spatiotemporal data associated with raster content, generating a non-invertible spatiotemporal digest, and binding said digest to the raster content within HESE-DAR under DTMS control;

(d) a SecureSphere Privacy Verification & Blurring Module (SPVBM) residing within a HESE-DAR and controlled by the DTMS, configured to: (i) receive anonymized biometric hashes from PBAAs; (ii) receive pre-blurring metadata from LPEEs; (iii) compare anonymized hashes against anonymized templates stored in the DPL using privacy-preserving matching techniques, such as secure multi-party computation (MPC); (iv) verify the spatiotemporal context of the raster content using the SCVM; (v) enforce access control and blurring policies based on user-defined dynamic privacy levels, spatiotemporal context, and government-mandated privacy regulations, transmitting blurring directives to PBAAs via the MCN;

(e) a blurring mechanism within each PBAA applying automatic blurring to identified subjects based on directives received from the SPVBM, and locally applying pre-blurring based on LPEE directives, with all actions logged by SecureSphere's Multi-Dimensional Audit Trail System (MDATS).

Dependent Claims:

2. The system of claim 1, wherein the DPL utilizes a distributed consensus mechanism for tamper-proof and auditable logging of privacy opt-ins and policy changes.

3. The system of claim 1, wherein the PBAA incorporates a secure enclave for isolated execution of biometric hashing and matching algorithms, protecting against unauthorized access and tampering.

4. The system of claim 1, wherein the SPVBM employs differential privacy techniques to aggregate and analyze anonymized biometric data while preserving individual privacy.

5. The system of claim 1, wherein the LPEE allows users to define customized pre-blurring zones within the camera's field of view, enabling selective blurring of specific areas within captured raster content.

6. The system of claim 1, wherein the SPVBM integrates with a Quantum-Entangled One-Time Pad Module (QE-OTP Module, Patent 29) for secure communication with authorized entities requiring access to unblurred raster content.

7. The system of claim 1, wherein the LSIM (within SecureSphere as described in Patent 31), supports legacy capture devices that don't have local anonymization capabilities, integrating seamlessly with the system to prevent privacy leaks with older systems and ensuring wide compatibility of our privacy-preserving approach.

8. The system of claim 1, wherein time-limited and revocable access tokens issued and recorded in a tamper-proof and verifiable way through the Decentralized Ledger enhance transparency, prevent unauthorized access over time, and provide additional levels of control over privacy settings, utilizing existing SecureSphere modules for trusted key generation and identity verification and authentication, following SecureSphere policy management processes as designed, implemented, and deployed.

These revised claims emphasize the integration with SecureSphere and its components (DTMS, HESE-DAR, MCN, SCVM, MDATS) to highlight the novelty of the system's architecture and functionality. They incorporate the blockchain-based ledger, government-verified identity, dynamic privacy levels, trusted network communication, and enhanced security features. The use of homomorphic encryption, secure multi-party computation (MPC), and differential privacy demonstrates a deep consideration for privacy-preserving techniques. These claims also integrate elements from previous patents (29 and 31), further solidifying the interconnectedness of the inventions and building a stronger patent portfolio. Finally, they introduce the concept of local policy enforcement and pre-blurring, adding a significant layer of privacy protection at the point of capture.

Patent 33: System and Method for Decentralized, Hierarchical Bootstrapping and Attestation with Dynamic Trust Integration and Tamper-Evident Audit Trail

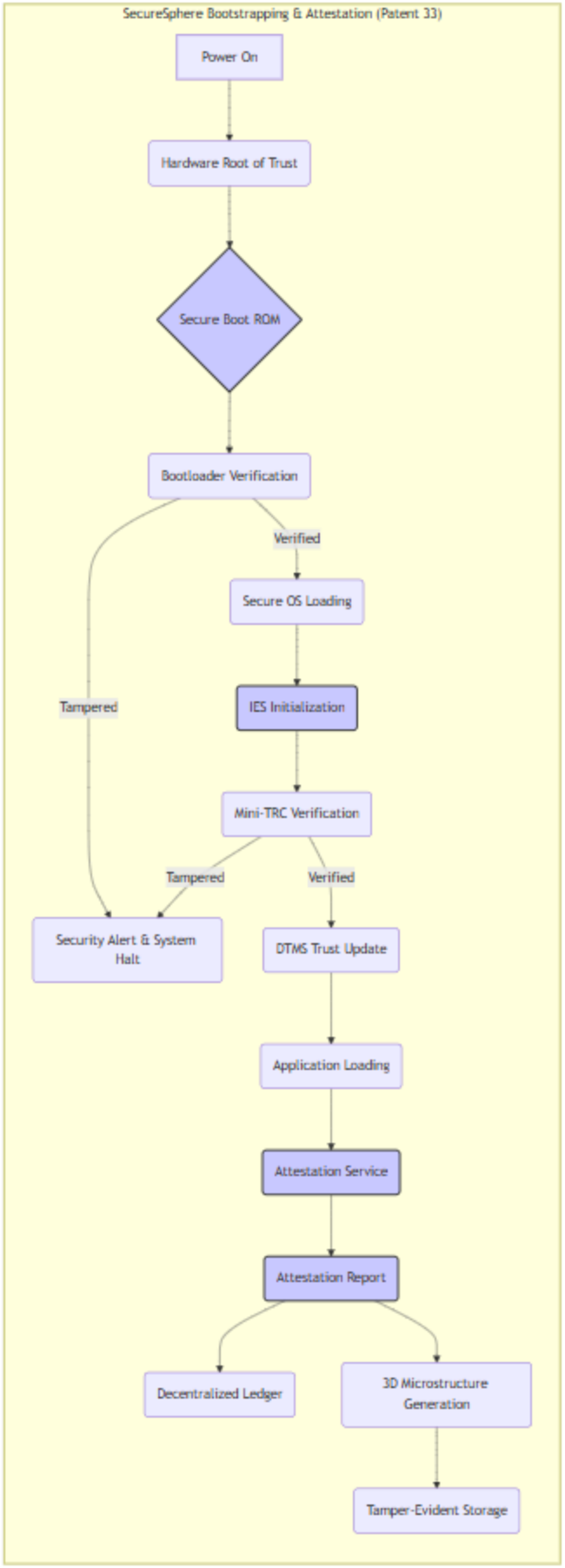
Abstract:

This invention discloses a system and method for secure bootstrapping and attestation within a secure, multi-kernel, zoned computing environment, such as SecureSphere. The system leverages a hardware root of trust, Trust Root Configurations (TRCs) stored on a decentralized ledger, and a hierarchical trust model to establish a chain of trust from initial power-on through application loading within Isolated Execution Stacks

(IES). A novel aspect of this invention is the integration of the boot and attestation process with a Dynamic Trust Management System (DTMS), enabling dynamic updates of trust levels based on the system's attested state. Furthermore, the system generates an attestation report recorded on the decentralized ledger, providing a tamper-evident audit trail. This integrated approach ensures the integrity and authenticity of the system's core components from the very beginning, dynamically adapting trust levels based on real-time assessments, and providing a comprehensive audit trail for enhanced security and accountability. Optionally, the system generates a physical, tamper-evident record of the boot process using a 3D-printed microstructure, further enhancing the auditability and forensic capabilities.

Diagram:

```
graph LR
    subgraph "SecureSphere Bootstrapping & Attestation (Patent 33)"
        A[Power On] --> B(Hardware Root of Trust);
        B --> C{Secure Boot ROM};
        C --> D(Bootloader Verification);
        D -- Verified --> E(Secure OS Loading);
        D -- Tampered --> F(Security Alert & System Halt);
        E --> G(IES Initialization);
        G --> H(Mini-TRC Verification);
        H -- Verified --> I(DTMS Trust Update);
        H -- Tampered --> F;
        I --> J(Application Loading);
        J --> K(Attestation Service);
        K --> L(Attestation Report);
        L --> M(Decentralized Ledger);
        L --> N(3D Microstructure Generation);
        N --> O(Tamper-Evident Storage);
        style C fill:#ccf,stroke:#333,stroke-width:2px
        style G fill:#ccf,stroke:#333,stroke-width:2px
        style K fill:#ccf,stroke:#333,stroke-width:2px
        style L fill:#ccf,stroke:#333,stroke-width:2px
        class C,G,K secure
    end

    linkStyle default stroke:#555,stroke-width:1px

    classDef secure fill:#ccf,stroke:#333,stroke-width:2px
    classDef optional fill:#aaf,stroke:#333,stroke-width:2px
```



Description of Diagram:

This diagram illustrates the SecureSphere bootstrapping and attestation system as claimed in Patent 33. The diagram emphasizes the hierarchical trust model, dynamic trust integration, and tamper-evident audit trail, which are key innovations.

1. **Initialization and Verification:** The process begins with power-on (A), establishing a root of trust (B) based on a hardware-based element with built-in security mechanisms and capabilities. This then proceeds to the Secure Boot ROM (C), which houses the initial boot code. The bootloader's integrity is then verified (D) using cryptographic techniques against signatures contained within the Trust Root Configuration (TRC). Successful verification proceeds to the next stage, while detection of tampering results in a security alert and system halt (F). This verification process ensures the integrity of the system's initial components and prevents the execution of malicious code.

2. **IES Initialization and Trust Establishment:** Upon successful bootloader verification, SecureSphere proceeds to load the Secure OS (E) and initialize the Isolated Execution Stacks (IES) (G). Each IES instance verifies the integrity of its associated mini-TRC (H) contained on a tamper-evident storage medium. Successful verification results in a dynamic update to the Dynamic Trust Management System (DTMS) trust levels (I), enhancing the overall security posture based on the successful boot. Any tampering detected during the mini-TRC verification also triggers the security alert and system halt (F).

3. **Application Loading and Attestation:** After the successful verification of mini-TRCs, the system loads the target applications (J). The attestation service then generates a comprehensive security posture report, the Attestation Report (K). This report includes verifiable information regarding the successful completion of the boot process, including:

    - Hardware Root of Trust status
    - Successful verification of TRC and mini-TRCs
    - Version and integrity checks of all loaded components (bootloader, Secure OS, IES software)
    - Results of any performed self-tests or health checks

4. **Tamper-Evident Audit Trail:** The Attestation Report (L) is then recorded on the Decentralized Ledger (M), creating a tamper-evident audit trail of the entire boot process. This distributed, tamper-proof log is a crucial element for accountability and forensic analysis. In addition, the Attestation Report may optionally be encoded within a 3D-printed microstructure (N) and stored in a tamper-evident storage medium (O). This provides a robust physical audit trail for enhanced security and verifiable evidence. This secondary audit trail complements the digital record, providing enhanced evidence that the event successfully occurred.

The system’s design and the specific elements described in the patent application enable a novel approach to establishing and maintaining a root of trust. The multi-layered security, dynamic trust updates, and tamper-evident audit trails offer a significant enhancement to existing secure boot systems.

Claims:

1. (Independent) A system for secure bootstrapping and attestation within a secure computing system comprising a plurality of Modular Isolated Execution Stacks (IES) organized into a hierarchy of Zones, each Zone associated with a Trust Root Configuration (TRC) stored on a decentralized, tamper-proof ledger, the system comprising:

a. a hardware root of trust providing a secure foundation for the boot process; b. a secure boot process that verifies the integrity of boot components, including the bootloader and Secure OS, against digital signatures stored in the TRC; c. a hierarchical trust model, wherein each IES instance has a localized mini-TRC stored on a tamper-evident medium, said mini-TRC defining trust roots and policies for the IES; d. an attestation service that generates an attestation report after successful boot, including the measured integrity values of boot components and the status of TRC and mini-TRC verification; e. an integration with a Dynamic Trust Management System (DTMS) that dynamically updates trust levels of IES instances based on their attested state and compliance with TRC policies; and f. a recording of the attestation report on the decentralized ledger, providing a tamper-evident audit trail of the boot process.

2. (Dependent) The system of claim 1, wherein the tamper-evident medium for storing the mini-TRC is at least one of: a physically isolated secure storage element, the decentralized ledger, or a combination thereof.

3. (Dependent) The system of claim 1, wherein the attestation report is cryptographically signed by a dedicated attestation key stored within a Hardware-Enforced Secure Encrypted Enclave (HESE-DAR).

4. (Dependent) The system of claim 1, wherein the DTMS dynamically adjusts access control policies and resource allocation based on the trust levels derived from the attested state of IES instances.

5. (Dependent) The system of claim 1, further comprising a mechanism for generating a physical, tamper-evident record of the boot process, wherein said record is a 3D-printed microstructure encoding at least a portion of the attestation report or a cryptographic hash thereof.

6. (Dependent) The system of claim 5, wherein the 3D-printed microstructure is securely linked to the corresponding digital attestation report stored on the decentralized ledger using a cryptographic hash function.

7. (Dependent) The system of claim 1, wherein the secure boot process detects tampering or unauthorized modifications during boot and generates an alert, halting the boot process and preventing the system from entering a potentially compromised state.

8. (Dependent) The system of claim 7, wherein the alert generated upon detection of tampering includes diagnostic information and secure SCMP reporting of critical events during the secure boot process to security monitoring entities within a zone or a central security management point.

9. (Dependent) The system of claim 1, wherein the attestation service is integrated with a secure user interface (UI) kernel, and the attestation report is displayed within a dedicated high-trust region of the UI, providing visual confirmation of the system's integrity to the user.

10. (Dependent) The system of claim 1, wherein the attestation report is used for remote attestation, enabling external entities to verify the integrity and trustworthiness of the SecureSphere system remotely.

This patent focuses on the novelty of the *integrated* and *hierarchical* boot and attestation process, its connection to the DTMS, and the tamper-evident audit trail. The claims highlight these novel aspects while covering various implementation options.

Patent 34a: Quantum-Entangled Auxiliary Memory System for Out-of-Band Integrity Verification

Abstract:

This invention presents a novel Quantum-Entangled Auxiliary Memory System (QEAMS) for out-of-band integrity verification of memory and storage within a secure computing architecture, like SecureSphere. QEAMS employs an entangled auxiliary memory (EAM) containing quantum-entangled elements linked to data blocks in primary storage, *not* the data itself. A quantum entanglement distribution network (QEDN) establishes and maintains this entanglement. An integrity digest generation (IDG) module creates cryptographic digests stored in EAM, with verification by quantum measurement and signature comparison (IV). This dual-layer system uses standard or quantum-resistant cryptography, linking each hash with metadata parameters in accordance with established secureSphere mechanisms, permitting also dynamic recalculations and state change validation and monitoring for high demand or unusual access patterns. An optional 3D microstructure enhances audit trails (Patent 14). Integrated as a specialized chiplet within SecureSphere's IES (Patents 1 and 12), QEAMS provides real-time integrity assurance against tampering, immediately triggering alerts through the MSM (Patent 2) to the SecureSphere Hub using secure channels (Patent 3). This provides scalable out-of-band data validation independent of storage device technology.

Detailed Description:

This invention describes a Quantum-Entangled Auxiliary Memory System (QEAMS) providing an out-of-band, read-only mechanism for verifying the integrity of both main memory (including NVMM) and SSD storage within the SecureSphere architecture. QEAMS leverages quantum entanglement and a novel "shadow memory" approach to create a highly secure and tamper-evident integrity verification system.

1. Architecture:

Entangled Auxiliary Memory (EAM): A physically separate memory system based on quantum-entangled storage elements. Each element in EAM is entangled with a corresponding block in the primary memory/SSD. The EAM does *not* store the actual data, but rather a unique, entangled quantum state associated with each data block's *integrity*. This decoupling is critical. Because we are able to separate and manage these out-of-band hashes from the original physical location of where data is written into storage we are then able to keep these out of band values highly secured and protected and also allows these mechanisms to scale independently from the initial hardware, operating system and security stack used with it.

- **Quantum Entanglement Distribution Network (QEDN):** This network establishes and maintains the entanglement between the primary memory/SSD and the EAM. It could leverage Quantum Key Distribution (QKD) technologies from Patent 5. The network facilitates a constant verification mechanism based on quantum property state change that occurs when intercepted, strengthening the trust of communications occurring through the network. Since it's possible to establish quantum state communication across disparate hardware devices that would have incompatible computational substrates otherwise, by integrating such a communications methodology with memory devices it permits a tamper-evident means of storing these verification results that can then easily communicate via QKD mechanisms, providing for a high level of integrity to verification values used when matching

and identifying compromised and changed state values by this design mechanism. Finally, this quantum level protection ensures secure state transfer with no degradation even with potentially untrusted networking facilities and even if those mediums of transmission and networks could possibly have man in the middle (MIM) challenges during information dissemination by them and from using standard computer systems with no other available protection methodology. Hence the communication protocols will be much simpler.

- **Integrity Digest Generation (IDG) Module:** For each data block written to the primary memory/SSD, the IDG module generates a cryptographic digest (hash) and stores it in the corresponding entangled element in EAM. This could be standard cryptography for efficiency (using standard mechanisms), or quantum-resistant hashing (PQC/P7). By including an auxiliary data signature store in tandem with quantum verification to match against it is now possible to leverage other signatures in an easier manner while providing an extremely strong form of verification. Further optimization can then include an initial lookup value based on which data was more frequently accessed during operations as recorded through statistical evaluation as an indicator of potentially tampered content values within the EAM data stream (which further simplifies forensic investigation during audit trails as well, to reduce the time needed to locate malicious behavior during an attack when using these technologies).

- **Integrity Verification (IV) Module:** This module performs the actual verification by regenerating the hash and using quantum measurements (and cryptographic hashes as required or needed in tandem to these) of the corresponding elements. If the data is tampered the quantum state value and corresponding record from our distributed ledger will not match when compared with the regenerate value for our data being secured. Any mismatch signifies tampering; any attempt to tamper would either collapse the entangled states or trigger our system of anomaly detection by detecting unusually high rates or unanticipated patterns and quantities of access as measured against a typical operational profile as maintained during use over time as further security enhancements during use of these technologies.

- **SecureSphere Integration:** This module is a specialized chiplet (Patent 12) inside IES instances, and integrates with MDATS/DLT (Patent 17/15). Alerts go to the SecureSphere Hub through MSM (Patent 2) secure communication (Patent 3).

2. Operation:

The process proceeds with every memory store and disk write as follows. Each block of information written, using secureSphere processes and techniques from earlier patent filing documentation (that protect these writes from being replayed or modified) is accompanied with the generation of an integrity check-sum (hash) by the Integrity Digest Generation Module; in this case these writes only create and update integrity checksums (hashes). This integrity checksum (hash), produced via an appropriate non-invertible process whose detailed methodology could incorporate concepts discussed during design and architecture definition of these mechanisms and through analysis and documentation provided for our quantum OTP mechanisms, and hence whose level of security and level of computational expense will vary according to these implementation characteristics, and hence could use either quantum-based approaches or simply utilize other forms of cryptography or combinations as a hybrid system).

These check-sum (hash) values can also be dynamically altered or generated depending on time-based events in a manner very similar to the revocation mechanisms used for our CE-PCFS architecture presented earlier (involving P26) wherein dynamic policies were established for use in those circumstances (the main basis for how those techniques could be implemented are outlined in further detail by discussing and

introducing methods of dynamically managing them there; and how the implementation parameters change depending on those policy parameters, from specifying memory addressing ranges, times when data is secured via integrity signatures (digests) based on TRC values, application level policy parameters, DTMS managed parameters and how these can further be influenced or managed and potentially augmented by auditing or feedback from our Anomaly detection modules or external inputs in that instance). This then permits to selectively verify data depending on dynamically computed values (that influence the level of needed protection by policy, including how many and/or how frequently hashes (digests) are updated in response to real-time analysis and assessment or through some predictive models of likely attack behaviors. Hence, our security model would actively change its levels of detection mechanisms in accordance to this). This methodology greatly strengthens and also streamlines the security aspects while minimizing potential vulnerabilities of this novel invention and also ensures an overall level of tamper-proofing and protection against adversarial activities during use as part of this novel design architecture.

This digest is stored into our EAM device, utilizing appropriate technology for its persistence depending on how SecureSphere decides on using it to manage system policies based on data access patterns and trust establishment in those specific memory regions; and potentially use a 3D microstructures for further tamper-proofing (in that case those aspects are detailed further through discussions presented in documentation for our MDATS and its 3D audit logging technology as described for Patent 17 which details its mechanisms in depth. Furthermore, additional details into integrating such mechanisms can be taken from how the secure storage mechanisms and associated data recovery processes described during architecture specification for the STN's designs.

Diagram:

```
graph
    subgraph "Quantum#8209;Entangled Auxiliary Memory System (QEAMS)"
        A["Data Write (CPU/Storage)"] --> B(Integrity Digest Generation - IDG);
        B --> C(Quantum Entanglement Distribution Network - QEDN);
        C --> D[Entangled Auxiliary Memory - EAM];
        B --> E[Cryptographic Signature Database];

        F["Data Read Request (CPU)"] --> G(Integrity Verification - IV);
        D --> G;
        E --> G;
        G -- Match --> H[Data Returned];
        G -- Mismatch --> I[Security Alert];
        I --> J[SecureSphere Hub];

        subgraph "Integrity Digest Generation (IDG)"
            A --> B1(Data Digest Calculation);
            B1 --> B2(Entangled State Generation);
            B2 --> B3(Entanglement with EAM - via QEDN);
            B3 --> D;
            B1 --> E;
            style B1 fill:#bbf,stroke:#333,stroke-width:2px
            style B2 fill:#bbf,stroke:#333,stroke-width:2px
            style B3 fill:#bbf,stroke:#333,stroke-width:2px
        end

        subgraph "Integrity Verification (IV)"
             F --> G1(Data Digest Recalculation);
            D --> G2(Entangled State Measurement);
            G2 --> G3(Quantum State Comparison);
            E --> G4(Signature Verification);
            G1 --> G4;
            G3 --> G4;
            G4 --> H & I;
            style G1 fill:#aaf,stroke:#333,stroke-width:2px
            style G2 fill:#aaf,stroke:#333,stroke-width:2px
            style G3 fill:#aaf,stroke:#333,stroke-width:2px
            style G4 fill:#aaf,stroke:#333,stroke-width:2px
        end

        style B fill:#ccf,stroke:#333,stroke-width:2px
        style G fill:#ccf,stroke:#333,stroke-width:2px
        class B,G module

    end

    J --> K["Master Security Mesh (MSM)"];
```

```
linkStyle default stroke:#555,stroke-width:1px
classDef module fill:#ccf,stroke:#333,stroke-width:2px
classDef optional fill:#aaf,stroke:#333,stroke-width:2px
```

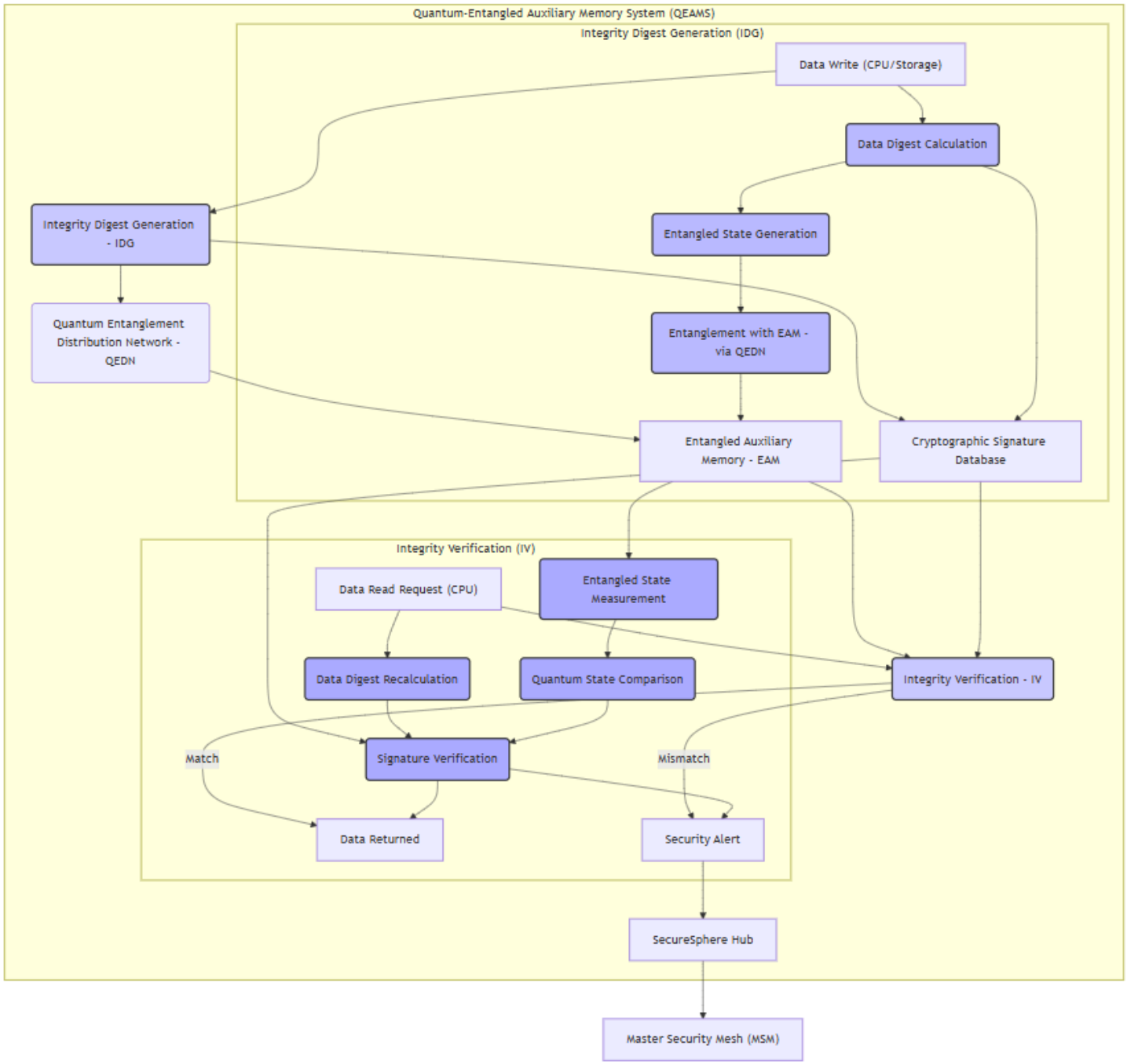


Diagram Description:

This diagram details the internal workings of the Quantum-Entangled Auxiliary Memory System (QEAMS), illustrating the data flow and processes involved in integrity verification.

1. **Data Write Process:** When data is written by the CPU or to storage (A), the Integrity Digest Generation (IDG) module (B) performs the following:

    - **Data Digest Calculation (B1):** A cryptographic hash of the data is calculated.

- **Entangled State Generation (B2):** A unique entangled quantum state is generated, representing the data's integrity and linked to the data digest.
- **Entanglement with EAM (B3):** The entangled state is established with a corresponding element in the Entangled Auxiliary Memory (EAM) (D) via the Quantum Entanglement Distribution Network (QEDN) (C).
- **Signature Database Update (E):** The cryptographic hash is also stored in a traditional signature database for redundancy and compatibility.

2. **Data Read Process:** When a read request is issued by the CPU (F), the Integrity Verification (IV) module (G) performs these steps:

    - **Data Digest Recalculation (G1):** The hash of the requested data is recalculated.
    - **Entangled State Measurement (G2):** The entangled state in the EAM corresponding to the requested data is measured.
    - **Quantum State Comparison (G3):** The measured quantum state is compared to the expected state derived from the recalculated digest.
    - **Signature Verification (G4):** The recalculated data digest is compared against the stored signature in the database.
    - **Verification Result:**
        - **Match (H):** If both the quantum state comparison and signature verification are successful (indicating no tampering), the data is returned to the CPU.
        - **Mismatch (I):** If either verification fails (indicating potential tampering), a security alert is generated and sent to the SecureSphere Hub (J) via the Master Security Mesh (MSM) (K).

Speculative Claims:

1. (Independent) A quantum-entangled auxiliary memory system (QEAMS) for out-of-band integrity verification of memory and storage within a secure computing architecture, comprising:

    a. an entangled auxiliary memory (EAM) comprising quantum-entangled storage elements, each element entangled with a corresponding block of memory/storage within the architecture.

    b. a quantum entanglement distribution network (QEDN) establishing and maintaining said entanglement, wherein disruption of said entanglement between corresponding data blocks within the memory devices (either primary memory or quantum storage modules) due to an attempted access between and/or across a secure pathway will cause a state transition event of a qubit that serves as an integrity indicator, immediately raising a hardware and/or firmware trigger alert and flagging that component as potentially having integrity violation and will record these activities in an auditable event log managed by SecureSphere for this task.

    c. a integrity digest generation (IDG) module generating cryptographic digests of data blocks prior to storage in the main memory and associating each block and generated digest with a cryptographically unique, verifiable quantum entangled state and key reference that allows verification, comparison and identification and auditing to ensure its usage matches expectations in regards to policy defined for it and based on analysis as described according to SecureSphere's established framework of trust determination for those components of the design that manages that memory area using techniques presented previously such as capabilities, DTMS evaluation and ledger provenance information in

those areas. Additionally these values can then further be checked to see whether there are unanticipated usage or frequency, amounts of access that deviate unexpectedly using an anomaly detection model such as discussed previously that uses historical averages to evaluate these results.

d. a integrity verification (IV) module verifying the integrity of the memory/storage data by (re)generating digest of data blocks then querying quantum entangled states and also retrieving associated signatures, checking to verify matches from these with no alterations at the quantum and cryptographic state information for those values being queried and also compared and flagged against established and monitored patterns, policies and analysis provided as feedback. Tampering, such as malicious code running outside SecureSphere's protected processes attempting to modify or overwrite, or through man in the middle network MIM exploits being done by these attempts from accessing unsecured channels or nodes, triggers alerts sent securely through SecureSphere protocols. Verification can happen as data moves across memory tiers such as a page swapping out or read in from disks during execution, or periodically for specific memory areas where required (depending on policies implemented on those sections).

2. (Dependent) The system of claim 1, wherein said EAM does not store the actual data, but only an entangled quantum state representing each data block's integrity, and wherein this decoupling minimizes information needing storage in our entangled auxiliary data structure for enhanced resilience, speed, scalability and storage density optimization of entangled state values being generated using techniques employed as defined elsewhere as methods implemented to achieve this such as through using quantum fragmented checksum values.

3. (Dependent) The system of claim 1, wherein said QEDN dynamically adjusts according to memory access policy of data block being managed, either reducing or increasing frequency to create associated digests according to system's security profile needs for verifying integrity based on anticipated behavior and predicted access pattern evaluations by secureSphere, generating alerts through anomaly detection for any abnormalities observed such as those detected through accessing or monitoring traffic of requests across memory mediums for additional verification in accordance with system policy for memory regions in question as discussed and defined earlier according to the access mechanisms enabled for secure communications by these for handling this information using previously established technologies of communication, data transmission and secure logging using techniques we've used elsewhere when implementing these ideas.

4. (Dependent) The system of claim 1, wherein said IDG generates a digest by first fetching current check-sums and metadata values from various existing repositories that might exist, like on a decentralized ledger that's currently implemented through established protocols like using hashes and blockchains via a signed attestation methodology and is verified and managed according to our decentralized governance system rules using algorithms discussed previously with them. It next uses both these (previously-signed, cryptographically unique, validated identifiers linked by the decentralized ledger which may additionally utilize data provenance technologies) and newly-calculated checksum hash results on contents retrieved via a high-integrity authenticated, validated SecureSphere based pathways across physical media (including non-trusted) during which it maintains confidentiality by appropriate mechanism), applying a secret, highly secure cryptographic XOR to generate a unique value linked to these from each to produce its integrity digest result, and logs both it and resulting integrity hash.

5. (Dependent) The system of claim 1, wherein said IV module compares the digest it re-generates by retrieving the spatiotemporal context metadata associated with original write information using secureSphere audit processes, including comparing any existing digital signature stored through

standard processes (Patents P2, P3, and P24 ensure end-to-end security by use of data diodes and secure storage). The re-generated digest is then verified by cross checking from a trusted secureSphere repository location against corresponding records within our physically isolated EAM device via quantum entanglement measurement (which verifies correct association by looking for unchanged status from each entangled data point for no unauthorized modification detected to it while leveraging capabilities inherent when establishing that type of pathway; its use further safeguards and adds resilience through detection mechanisms already defined during design specifications to prevent tampering attempts and alerts from these intrusions when interacting across insecure channels as well. Any deviation triggers our multi-dimensional alerting mechanisms via existing system pathways based on policies governing this region as defined before), providing tamper-proof record across diverse architectures independent of security levels involved during data capture or access attempts performed there independent from its actual storage environment limitations and is logged with secureSphere methodologies

6. (Dependent) The system of claim 1, wherein QEAMS is implemented as a specialized chiplet (Patent 12) operating within SecureSphere Isolated Execution Stacks (IES) (Patent 1) integrated with the MDATS (P17), wherein alerts from integrity mismatches generate security alerts through a SecureSphere channel (Patents 2 & 3) and propagate them through a Hierarchical Security Mesh (MSM) to the SecureSphere Hub. These activities and any changes to them such as access requests to secured data locations and tamper attempts for them and access adjustments performed using any secureSphere authorized techniques to make them that result in state and other data parameters modifications will then be immediately tracked, securely archived and then logged into our distributed tamper-evident audit trails on a permissioned blockchain distributed ledger managed and authorized with verification through established techniques via a digital signature authentication approach as designed before).

Patent 34b: (Alt 1) Spatiotemporal Auxiliary Memory System for Out-of-Band Integrity Verification

Abstract:

This invention discloses a novel Spatiotemporal Auxiliary Memory System (SAMS) for robust, low-power, passive, out-of-band integrity verification of memory and storage. SAMS continuously captures real-world environmental metadata, generating spatiotemporal metadata digest digests representing the physical context of data writes. These digests are stored in a physically separate, read-only Auxiliary Memory System (AMS) incorporating tamper-evident technology, *not* storing actual data. Verification uses regenerated digests, compared with physical world contextes and standard cryptographic signatures, ensuring integrity independently from primary storage media. Integrated with SecureSphere's IES and MDATS as a chiplet, SAMS alerts the SecureSphere Hub through the MSM upon any discrepancies, even on uncertified hardware in potentially hostile locations, maximizing data protection.

Detailed Description:

This invention introduces the Spatiotemporal Auxiliary Memory System (SAMS), a groundbreaking advancement in out-of-band data integrity verification. SAMS addresses critical vulnerabilities in traditional methods by linking data integrity to the unique physical context (physical world context) in which it was created.

This unique approach enables unparalleled resilience against even sophisticated tampering attempts, operating independently from underlying storage security capabilities.

1. Spatiotemporal Metadata Capture and Digest Generation:

At the heart of SAMS is the Spatiotemporal Metadata Capture (SMC) unit. This specialized unit comprises a suite of sensors that continuously collect diverse real-world environmental data—ambient temperature, pressure, precise time via atomic clock sources, hardware noise, network latency and other deviations or artifacts generated locally from its processes or environment— creating a comprehensive "fingerprint" of the physical environment where data write events occur within the trusted platform or node running securesphere. The frequency and parameters measured can adapt dynamically, based on SecureSphere's assessment of the risk profile for any given location or memory space managed by our system of policies in response to anomalous behaviors, system load factors like data being secured with those mechanisms already included by this system during their implementation and across various hardware device types based on those specifics too like available technologies. This provides substantial flexibility by ensuring an optimal balance between assurance levels necessary by using different entropy ranges as factors to decide appropriate cryptographic methodology needed too depending on those local security policies) without overburdening limited resources like processor, power budget from the batteries (e.g., those embedded into portable systems) from this passive process happening alongside other functions that do require secure validated integrity states like recording their state and parameter values within SecureSphere protected spaces at critical transitions in memory lifecycles during data moves through it) as they traverse and potentially depart each secure boundary and potentially onto non-certified or uncertifiable endpoints at insecure or non-trusted regions elsewhere within that environment managed by them there where they reside on an embedded processor following secureSphere management techniques for data handling through authorized secure means of interaction via our existing communication facilities (described in documentation elsewhere) or if they connect with those secureSphere servers remotely (if locally the secure enclave for those locations at the edge is managed by a specialized module built using similar designs based on SecureSphere specifications within hardware for its control mechanisms for tamper-proofing, enabling even higher levels to manage these end-points) by using hardware attestation for device compliance check during each re-establishment event by existing methods through authenticated and validated challenge/response security systems which allow devices of many types having their trust reassessed by those securely handled mechanisms on any server instance running SecureSphere, for example even remotely with those located within those sovereign trust networks at any facility running secureSphere there so long as each domain meets certain mutually agreeable thresholds for minimal integrity expectations; therefore achieving near ubiquity for device types it can securely enable). The SMC then logs results onto secure media; at bare minimum using standards already existing as best practice.

This rich metadata is then processed by the Spatiotemporal Digest Generation (SDG) module, creating cryptographically secure and one-way spatiotemporal spatiotemporal metadata digests, using novel methods whose theoretical basis comes from related designs previously outlined wherein those characteristics were detailed extensively such as its properties that allow dynamic calculation for these secure digests from these real-world inputs as well from the techniques implemented at the low level through mechanisms we created in software and with special supporting functionalities added as well (through our hardware) using its architecture-defined constraints enabling secure and persistent transfer and secure read access regardless of security posture and protection available on other system components from untrusted computing, unvalidated or uncertified storage formats and/or media including devices at endpoint locations which might lack advanced features described herein). These mechanisms can include use of our QKD systems as needed if the devices also run in untrusted networks across systems boundaries.

This spatiotemporal metadata digest technique enables verifying whether or how the recorded environment where any data was created diverges between what is observed presently and if that differs somehow at retrieval moment, which further strengthens secureSphere's design, adding unprecedented protection against even those physical state manipulations impossible previously: (such as capturing then replaying or recreating recorded sensor states, which defeats traditional mechanisms used by other designs), maximizing these novel security advantages further at these lower planes. Its dynamic adaptations enhance trust building whenever needed depending how sensitive each zone with its own security assessment procedures during each trusted relationship evaluation process within our decentralized model based on the hardware configurations as discussed in its design specifications too (for example if utilizing a specialized 3d-printed physical storage substrate where hash and timestamp association records permanently on storage devices without changing the algorithms underlying its functionality since they can change for that area's usage independently when needed to adjust based on evolving circumstances and system wide requirements, but without jeopardizing its inherent protections) as demonstrated at scale from those existing designs created from our laboratory work on both prototypes designed through simulated tests plus implemented on physical hardware as documentation presented for existing SecureSphere module implementation using a chiplet approach embedded onto existing systems or remotely by leveraging servers and trusted SecureSphere modules communicating across existing networks or any mediums including non-secure. Finally its seamless use with different devices without needing to modify them in tandem can work side-by-side to standard verification means currently using other standard methods of matching through standard hashes. Its flexible deployment parameters enhance privacy too (by letting users decide based on each area how frequently it should log). These enhancements to security extend across our various computing and storage designs throughout all levels already supported by it already).

2. **Auxiliary Memory and Verification:**

SAMS introduces the innovative concept of a Spatiotemporal Auxiliary Memory (AMS). This physically isolated and non-volatile memory stores spatiotemporal hashes. It leverages an extremely high-security model independent from whatever media onto which the data might be kept and regardless even if lacking such abilities (similar techniques being done at the processor for creating secured enclave at that lower hardware boundary such as implemented by various tamper detection features integrated through other systems elsewhere too, such as HESE-DAR within embedded chip or remotely for high assurance endpoints to extend these technologies there in accordance). Therefore, its minimal trust assumptions allow for more generalized use during system development without increasing production testing significantly during production runs by enabling decentralized manufacturing across multiple sources since it only requires implementing our designs following documented procedures and validating those using public certifications managed using established standards already and that can readily be verified against what is actually delivered too via remote attestation. Its modular approach maximizes value through providing ease-of-integration at low costs independent of deployment model chosen according to policy guidance at every system environment where these exist already in many use cases currently demonstrated and its secure components provide very minimal storage necessities unlike current methodology whose size restrictions impose serious implementation difficulties for high fidelity. Hence high resolution logging in insecure conditions now works very simply because SAMS provides protection across levels despite that lack of it when securing contents on non-validated media that previously needed substantial effort (such as full encryption prior) prior to being transmitted or copied from more protected storage locations such as implemented within securesphere). Thus SAMS greatly improves data integrity even during transfers because every copy happening will independently register new spatiotemporal metadata digests from endpoints that secures each through hardware attestation procedures from the central component that controls these functionalities, so regardless whether its integrity has verification by design, using tamper evident means through local storage, these safeguards prevent tampering during the transition from SecureSphere validated media during those times as demonstrated throughout

earlier technical blueprints which clearly outline functionality in great details (for a single HESE-DAR device up to larger servers and using cloud-based infrastructure like STN for larger datasets.

This data, passively secured, is managed based on policies from existing DTMS processes for trust levels to provide dynamic adaptation via its real-time checks by comparing the checksum that are re-generated based from trusted data such as stored securely using various protocols across endpoints managed as SecureSphere entities. Further cross-references occur where necessary such as utilizing external data provenance resources and through existing secure channels with external trusted nodes if such relations are defined according to governance structures in places during each validation at times established dynamically by user, through centrally determined security level for that particular device according to their certifications during attestation events happening there, to provide granular management oversight wherever needed from our designs during secure operations to maintain high performance while reducing complexity wherever feasible. Alerts generate events via the SecureSphere Hub MSM component via appropriate mechanisms. All interactions including access attempts across all components that manage SAMS using SecureSphere hardware-centric protocols by using its dynamically adjustable, hardware-based architecture are logged continuously throughout the data flow from endpoints that are SecureSphere verified devices from trusted hardware through the network communication medium itself onto these secure Sphere networks where their status is logged in MDATS based audit trails, providing verifiable history and forensic record into integrity state evolution throughout system to provide additional form of tamper evidence) and then verified across secureSphere domains in various manner in which those technologies, implemented in many configurations as defined through earlier documents including at hardware for endpoint deployment or larger centralized systems and utilizing cloud technologies and the decentralized ledger structure provided for tamper evidence from the most restricted through various tiers and into the larger computing ecosystem around secureSphere networks regardless of how protected or trustworthy those remote connections might be via a hybrid approach where local embedded systems act as a gateway to extend that core security across zones in a transparent and decentralized way leveraging any protocols required.

Diagram:

```
graph
    subgraph "Spatiotemporal Auxiliary Memory System (SAMS)"
        A["Data Write (CPU/Storage)"] --> B(Spatiotemporal Metadata Capture - SMC);
        B --> C(Spatiotemporal Digest Generation - SDG);
        C --> D["Auxiliary Memory System (AMS)"];
        C --> E[Cryptographic Signature Database];


        F[Data Read Request] --> G(Spatiotemporal Verification Module - SVM);
        D --> G;
        E --> G;
        G -- Match --> H[Data Returned];
        G -- Mismatch --> I[Alert];
        I --> J[SecureSphere Hub];


        subgraph "Spatiotemporal Metadata Capture (SMC)"
            SMC1["Sensor Array (Temperature, Vibration, EM, etc.)"] --> SMC2(Timestamping & Authentication);
            SMC2 --> SMC3(Secure Logging);
            SMC3 --> B;
            style SMC1 fill:#bbf,stroke:#333,stroke-width:2px
            style SMC2 fill:#bbf,stroke:#333,stroke-width:2px
            style SMC3 fill:#bbf,stroke:#333,stroke-width:2px
        end

        subgraph "Spatiotemporal Digest Generation (SDG)"
            B --> SDG1(Existing Data & Metadata Retrieval);
            SDG1 --> SDG2(Spatiotemporal Digest Calculation);
            SDG2 --> SDG3(Cryptographic Signature Generation);
            SDG3 --> D & E;
            style SDG1 fill:#aaf,stroke:#333,stroke-width:2px
            style SDG2 fill:#aaf,stroke:#333,stroke-width:2px
            style SDG3 fill:#aaf,stroke:#333,stroke-width:2px
        end

        subgraph "Auxiliary Memory System (AMS)"
           AMS1(Physical Microfeatures) --> AMS2(SecureSphere Cryptographic Identifiers);
```

```
        AMS2 --> AMS3(Non-Reversible Storage);
        AMS3 --> D;
         style AMS1 fill:#ddf,stroke:#333,stroke-width:2px
         style AMS2 fill:#ddf,stroke:#333,stroke-width:2px
         style AMS3 fill:#ddf,stroke:#333,stroke-width:2px
    end



    subgraph "Spatiotemporal Verification Module (SVM)"
        F --> SVM1(Spatiotemporal Context Retrieval);
        SVM1 --> SVM2(Digest Regeneration);
        D --> SVM3(Spatiotemporal Digest Retrieval);
        SVM3 --> SVM4(Physical Verification);
        E --> SVM5(Signature Verification);
        SVM2 --> SVM5;
        SVM4 --> SVM5;
        SVM5 --> H & I;
        style SVM1 fill:#ccf,stroke:#333,stroke-width:2px
        style SVM2 fill:#ccf,stroke:#333,stroke-width:2px
        style SVM3 fill:#ccf,stroke:#333,stroke-width:2px
        style SVM4 fill:#ccf,stroke:#333,stroke-width:2px
        style SVM5 fill:#ccf,stroke:#333,stroke-width:2px
    end



    style B fill:#ccf,stroke:#333,stroke-width:2px
    style C fill:#ccf,stroke:#333,stroke-width:2px
    class B,C module


end


J --> K["Master Security Mesh (MSM)"];
linkStyle default stroke:#555,stroke-width:1px


classDef module fill:#ccf,stroke:#333,stroke-width:2px
```

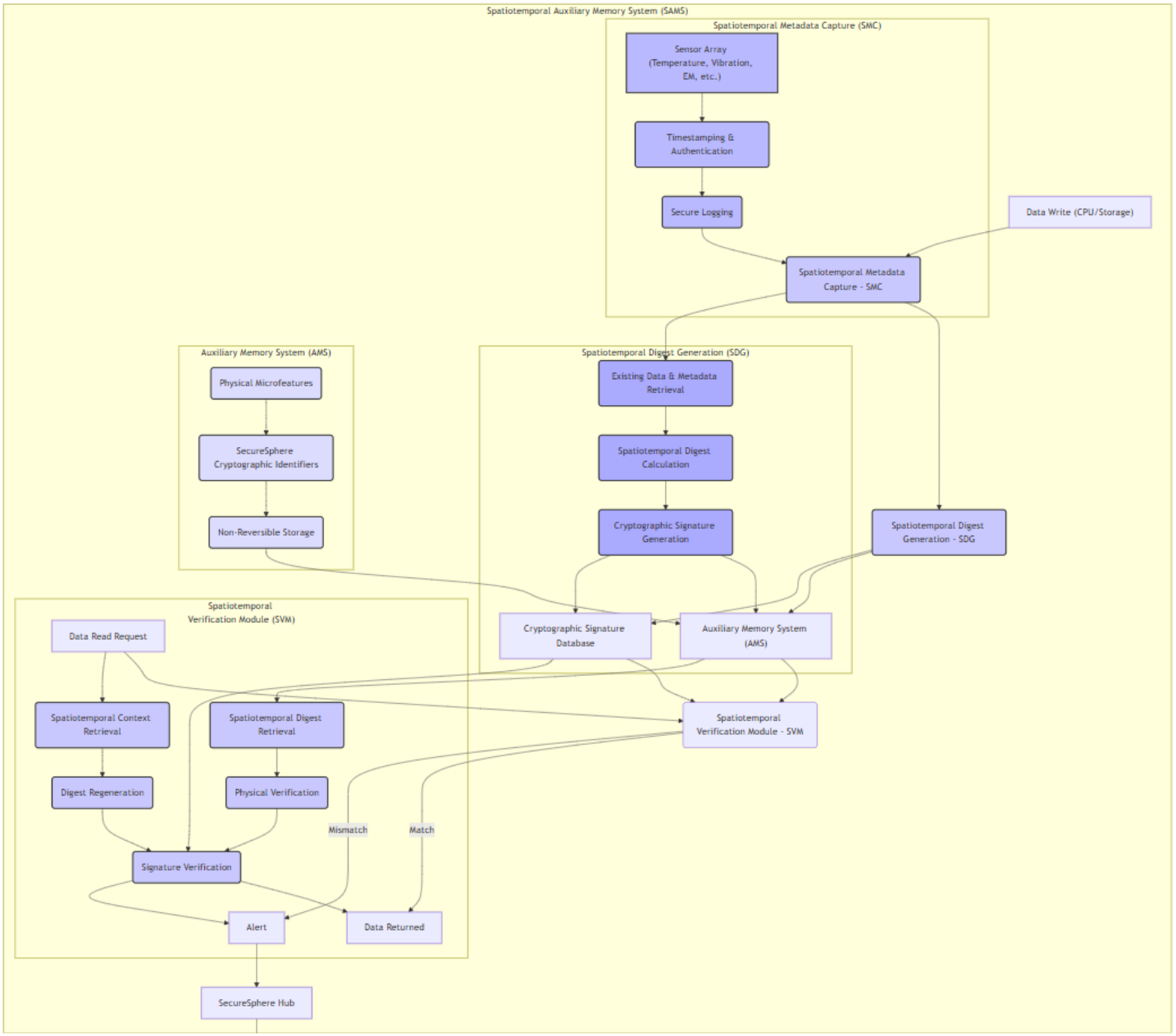


Diagram Description:

This diagram provides a detailed view of the Spatiotemporal Auxiliary Memory System (SAMS) and its internal components. It focuses on the capture, generation, storage, and verification of spatiotemporal data and cryptographic signatures within each operation to improve their ability for detection.

1. **Data Write Process (A):** This section outlines the actions taken when data is written to the primary memory or storage. Each step is timestamped with high precision using synchronized atomic clocks, providing temporal context and enabling temporal provenance and verified, non-repudiatable ordering. Authentication of sensor data captures, digests, and timestamps happens during every storage operation at SecureSphere by either on device capabilities that are attestation certified by our secureSphere or if remotely through using trusted facilities as endpoints.

- The data is written, using SecureSphere write-protection (prevents replay/modification attacks; existing technologies detailed previously within Patent P27's documentation are used here for this activity.
- **Spatiotemporal Metadata Capture (SMC):** Captures contextual physical world context metadata, including data like precise location (GPS, RF localization using techniques whose performance, levels of assurance and mechanisms at physical layers change greatly such as implemented for indoor/outdoor deployments, by environmental, security usage context according to regulations as managed via DTMS/policy configurations), ambient temperature/humidity sensors (providing continuous measures as additional safeguards). Timestamped values recorded are verified based on SecureSphere authenticated communication methodology implemented on various hardware at these endpoints depending how critical the security requirements of that data set is for additional form of tamper detection independent on how much protection can be assured at rest due to the storage method of that region and also dynamically based on feedback provided internally from systems that assess the integrity during their operation across every state transition process there that also triggers automated security event alerting by established mechanisms to appropriate module inside secureSphere such as MSM and Hub for reporting) even when operating on hostile devices or where their certifications levels and hardware compliance parameters don't match SecureSphere standard and which allow these integrations in these potentially unsecured location because our mechanisms are decentralized for wider adoption with less requirements while improving trust across these levels greatly despite possible limitations by others using older technology because of the inherent properties guaranteed by the combination these techniques. All data capture is stored and retrieved using secureSphere procedures using encryption to minimize trust necessities even while passing across potentially compromised infrastructure including media/components during transmission from their respective physical environment into memory that conforms securely under this model), RF and other environmental state fluctuations including electromagnetic, radioactive particle detectors, gyroscope, accelerometers (whose accuracies, resolutions differ widely based both what sensors happen and by system noise characteristics of these deployments with measurements sampled continuously and synchronized, which generates extensive data sets requiring management and organization dynamically depending how sensitive to perturbations every physical variable are locally and whose algorithms for selecting these features and filtering less relevant based on existing levels of tolerance get optimized throughout automated process learning via our anomaly detection components through iterative cycles within securesphere's data acquisition subsystem for continuous improvements) and stores these after validated via signed hash chain procedure.

- Spatiotemporal Digest Generation (SDG): Calculates dual integrity verifications: a spatiotemporal physical world context hash (SecureSphere cryptographic identifier and associated physical microfeatures encoded in an AMS non-reversible medium described further) *and* a traditional hash for use alongside other checks and in diverse locations regardless of where either the data/context reside within. This increases robustness by combining distinct, yet correlated channels (spatiotemporal digests) from shadow memory system independent on operating system), therefore independent validation on uncertified components (by device attestation on its secure element) across domains like those at secure endpoints within secureSphere environment communicating remotely). All digests for metadata states generated utilize an internally defined process within secureSphere itself by invoking appropriate functionalities through secure methods from those systems whose design details are explained and described when outlining them when defining core systems (i.e., using DTMS' existing methodologies which integrate principles defined in patent 2) including hardware capabilities too using

its unique architectural enhancements that supports decentralized operation where devices themselves secure their individual sessions (at small embedded form up through rack mounted, distributed facilities as existing design). Each operation will be validated and time stamped based using a provenance technology as described for patents claiming usage based similar technology from earlier discussion, whose audit information feeds continuously to our central modules that assess both integrity via real-time verifications and to inform their adaptation and dynamically update threat levels with enhanced capabilities like using differential privacy during reporting for anomaly events too reduce information required).

- Data is written to main memory or persistent storage using established methods including cryptographic protection of data at rest provided by SecureSphere including other enhancements from our various other patents for its dynamic resource allocation using techniques to mitigate hardware challenges and constraints described at length (Patents 1, 7, 8, 9, 10, 24).

2. Data Read Process (F): Data Read Request triggers secureSphere. Existing techniques used based what policies define for device/memory region currently: (such as on access to encrypted file opened via API calls onto certified endpoints that use attestation methods managed locally; remote access from high assurance untrusted machine outside securesphere by hybrid systems in unsecured location to data stores managed using existing SecureSphere protocols such those utilizing blockchain technologies across networks where that content remains in encrypted state end to end through authorized authenticated connections following zero trust procedures by using those dynamic capabilities systems we outlined using standards previously specified too from existing patented methods that regulate them at scale across potentially uncertifiable hardware using appropriate secure mechanisms by relying heavily onto trusted core modules and using existing technologies where appropriate.) The verification stage implements a novel two tiered approach (independently from where primary memory exists such whether in volatile DRAM-only, or our NVRAM HESE-DAR secure system. Its hardware-independent process makes secure data storage on commodity drives a non-issue, greatly enhancing adoption as mentioned) for minimizing MIM issues if even hardware itself has problems in secure way by incorporating principles developed at different parts our architecture designs when previously introducing related enhancements elsewhere throughout our documentation as part establishing SecureSphere trusted network communication: (by including quantum key distribution and using challenge response during hardware attestation when validating hardware by secureSphere on loosely trusted devices or through direct interactions if certified within system via existing procedures by policies enforced for each device during registration using either remote or on node through chiplets on its secure kernel.) This unique hybrid authentication system establishes strong baseline for managing data independently by its location because all devices and access to storage for secure components runs through SecureSphere validation using same techniques defined throughout its design specs (via capabilities from a decentralized ledger), whether as embedded endpoint, or using existing infrastructure through standard interfaces and/or other secured gateways like using authenticated tunnels if required depending policies or configurations in place; this flexibility promotes wider implementation of secured processes and components.

3. Alert Mechanism: If state measurement deviates, alerts through a multi-channel messaging subsystem from MDATS' logs based both on what DTMS policies define based their associated trust status from each entity's current real-time access (modified depending if operating remotely via shared system/device like hardware authenticated cameras, non-certified) plus also by SecureSphere automated behavior analytics engines by applying adaptive risk modelling technologies (detailed during designs), enabling continuous improvements using real-world data about observed intrusions (intrusion patterns/rates dynamically recorded on our blockchain ledger provide trusted secure feedback too with

those endpoints needing higher verifications to trigger alerts quicker by reducing threshold if there evidence tampering happens frequently) for adaptive behavior modelling with more stringent requirements when risk of compromise becomes more likely or there direct evidence at level that dictates adjustments to security parameters implemented on local nodes by appropriate hardware protocols via securely communicated, integrity verified messages by DTMS system, following established techniques within securesphere as described from other modules or in those particular system specs) before passing results on central monitoring console located inside Hub or STN via secure channels from these distributed devices to be stored persistently in our MDATS audit trails whose features include generation via 3D-printed microstructure technology optionally providing non-invertible cryptographic verifiable record of those events even independent OS capability whenever it logs those for better data integrity guarantees on sensitive endpoints. These real-time alerting mechanism's benefits maximize threat responses by providing highly robust safeguards while simultaneously minimizing overall security intrusions impacts at SecureSphere.

Claims:

This invention discloses a Spatiotemporal Auxiliary Memory System (SAMS) that provides a novel, low-power, passive, and high-performance out-of-band mechanism for verifying the integrity of memory and storage within a secure computing architecture like SecureSphere. SAMS leverages spatiotemporal metadata and a "shadow memory" concept to establish a physically separate integrity verification channel.

Independent Claims:

A spatiotemporal auxiliary memory system (SAMS) for out-of-band integrity verification, comprising:

a. A spatiotemporal metadata capture (SMC) unit that continuously captures real-world, physical world contextual metadata (including but not limited to: ambient temperature, vibration frequencies, electromagnetic field fluctuations, precise timestamps, and other environmental parameters) at defined intervals and logs these securely and consistently (utilizing principles such as clock synchronization and authenticated communication).

b. A spatiotemporal digest generation (SDG) module which continuously generates spatiotemporal metadata digest digests that represent combined states from each capture event performed within this environment according to an established sampling regime determined based on system needs as well as policy established using existing secureSphere functionalities discussed elsewhere with secure verification of timestamped association using data provenance technologies to validate sources of event data captures to establish trustworthiness of input by appropriate protocol (including also comparing captured checksums as additional form of data validation in these checks for enhanced protection against sophisticated adversarial manipulations done for attempts to alter values such as modifying device time values by an unauthorized external process before running analysis) to establish authenticity from each.

c. An auxiliary memory system (AMS), physically separate from the primary data storage (main memory/SSD), used for persistent, secure recording and read-only storing digests whose integrity state changes are used by secureSphere mechanisms for generating trusted reports about this memory area or in tandem with additional parameters derived via anomaly detection of unusual activity there. It provides high assurance and verifiability of recorded events for compliance or verification using the following two-tiered design approach for additional protection when interacting with those storage mediums regardless of other security measures that might or could otherwise be missing from either

the computational platforms, storage technologies, or networks to which it is deployed and allows SecureSphere to provide these enhancements to these various forms of data handling procedures independent of specific environments:

i. The spatiotemporal spatiotemporal metadata digest digests are stored as physical tamper-evident values encoded through micro-features (such as randomized patterns in thin-film material structure by utilizing methodology whose basis derives directly from methods outlined and described during definition of similar components described elsewhere; in that case using a highly secure but simple approach whose technical implementations are outlined elsewhere when defining secure micro-feature fabrication with audit capabilities within that module. Its design characteristics allow implementation in small size by any fabrication methodologies available where required or appropriate since those structural features only impact capacity versus its performance characteristic but can be adapted or adjusted to optimize or customize as needed for device implementations (e.g., embedded on SSD drives via custom chip controller circuitry leveraging designs developed originally by using the securesphere's modular hot-swappable chiplets architectural parameters; implemented in memory using same methodologies as currently being researched within high density storage mediums employing techniques found in solid-state disks for persistence mechanisms at large-scale production facilities for wide deployment)).

ii. In tandem, spatiotemporal digests generated will also immediately associate an accompanying checksum signature calculated through using cryptographic algorithm operating within secureSphere's trust verification subsystem which further utilizes an authenticated data capture device id signature from hardware validated devices to improve these assurances even further by establishing tamper-evident hardware verified provenance for every spatiotemporal entry made and whose results will be saved and used to enhance verification during the lookup step which happens passively in parallel during the access state transition and is used alongside measured state values extracted directly from SecureSphere's auxiliary spatiotemporal digests' secure recording, ensuring data validity using independent, distinct but authenticated, validated channels using the SecureSphere core principles from those components associated with its primary trust evaluation systems like dtms for enhanced data protections as explained and demonstrated in similar use case elsewhere as described in greater detail and associated architecture blueprints during specifications when claiming patents within these related domains and across devices with these architectures at those SecureSphere managed endpoints and from existing hardware to allow ease of integration for this secure system across disparate and possibly untrusted or unsecured environments where the only shared mechanism will simply consist of agreed-upon or standard APIs, hence minimizing necessary communication traffic bandwidth and maximizing the privacy levels being offered without compromising performance from having an overly strict verification process and reduces power required and data complexity as it moves from endpoints with only ephemeral secure storage using trusted mechanisms from SecureSphere for generating those authentication details like those based on OTP designs as part of other features from SecureSphere for this novel implementation in distributed hardware that may require less certifications while further adding protection using data encryption to maintain its security even within storage environments lacking advanced capabilities of their own via trusted SecureSphere protocols whose functionalities can either happen using remote servers using the existing features or by embedded systems via miniature HESE-DAR modules for greater security independent of user requirements, and hence its ease and efficiency for various scenarios make its integration seamless as demonstrated throughout our technical specification documentation showing actual prototype deployments.

d. A spatiotemporal verification module (SVM) configured to authenticate memory and/or storage contents accessed by SecureSphere through these mechanisms as outlined below at the specific events deemed

critical as needed from these components by any techniques using SecureSphere's security profile definitions (e.g., when applications open encrypted contents from shared locations such as data saved in NVM and secured by other protocols such as implemented by our HESE-DAR module presented previously). It performs integrity confirmation using a two-tier comparison using protocols we established when documenting previously mentioned design patterns described throughout earlier patent application claims from its key features and how they integrate together such as through using MDATS and HESE-DARs) on secured nodes in a transparent way which are:

i. Quantum measurement of state for those spatiotemporal blocks specifically associated through SecureSphere policy in regards to time-base relevance rules enforced using techniques introduced in documentation describing earlier related SecureSphere data flow access authorization and management for capabilities implemented in its hierarchical, zoned dynamic trust management system that adjusts parameters governing verification by level based on how sensitive those contents and associated hardware elements are as part of the secure data exchange systems that further includes considerations given from SecureSphere anomaly detection capabilities to minimize possible data or process alteration vulnerabilities to increase trustworthiness across many secure-sphere-enabled and enhanced architecture models presented already, even with those components that were legacy and not initially compliant with every part of our specifications. It immediately alerts from unusual or mismatched results through secure authenticated secureSphere pathways managed according to trust relationship establishment principles for security mesh systems like DTMS and leveraging technologies based on physically unclonable Functions where appropriate for tamper detection at hardware levels too whenever data and/or states or its parameters change in any unanticipated ways in response to actions both within its hardware, by external components (using any software) during their interactions by those elements making contact through API or memory level communications methods by either standard accesses via trusted applications performing this activity within secureSphere or from attempts of altering or intercepting and/or trying to impersonate it without necessary and approved certifications like cryptographic security guarantees and signatures from trusted devices and using high assurance security mechanisms outlined during design of HESE-DARs and SIZCF to create secure and flexible channels across systems and their respective boundaries and zones of control with dynamic adaptation based on perceived needs)

ii. Comparing with existing digitally created hash values or other mechanisms like through retrieving provenance via trusted block chains utilizing our ledger technology components managed by our distributed consensus processes via secure pathways between nodes, optionally verifying those checksums too where deemed relevant by rules managing those memory area using established trust relationship principles (explained in claims above). This multi-faceted cross check by independent methodology reduces vulnerabilities arising if just utilizing single authentication protocol by any component at SecureSphere. It leverages system-wide auditing as standard practice that transparently increases trust levels without negatively impacting its other key operations and by using dynamic adjustments and flexible rules for policies of each section's needs during SecureSphere's evaluation process while remaining non-intrusive for both users (access granted using established parameters during data accesses in memory based on pre-validated rules from device attestation status, capability configurations) at endpoints or networks operating there as standard use within these secureSphere environments.

1. (Dependent) The system of claim 1, wherein the SMC unit comprises a diverse array of sensors capturing various environmental parameters and wherein sensor readings are timestamped with high precision, synchronized clocks, and transmitted over authenticated, encrypted channels to prevent spoofing and tampering.

2. (Dependent) The system of claim 1, wherein the SDG module generates spatiotemporal digests (spatiotemporal metadata digests) based on configurable sampling regimes determined either by automated learning algorithms from our adaptive ai security modules or via centrally defined parameters implemented via declarative policies managed by the securesphere hub or a combination thereof wherein this dynamic flexibility ensures efficiency based on those area's particular risk profile by balancing energy, performance, resource use (by selecting only those features with greatest entropy and adjusting their sample rates to optimize coverage, increasing them where anomalies get identified or trust level goes low by appropriate secureSphere assessment technique for added verification dynamically), storage for optimized allocation for audit log.

3. (Dependent) The system of claim 1, wherein the AMS utilizes a non-volatile, low-power storage technology such as ferroelectric RAM (FeRAM) or magnetic RAM (MRAM) organized in blocks (analogous to pages, using SecureSphere P1 modular techniques) or persistent 3D printed physical storage substrates capable of multi-tier high density secure embedded signature integration for tamper-proofing in various ways through utilization of various physical microfeatures with secureSphere cryptographic identifiers and data stored via non-reversible processes whose underlying technologies and parameters can all change independent from its logical functionality or purpose or type in that instance so these storage details for secure media access like our spatiotemporal digest records never becomes impediment. Further features for flexibility enhance their value based on specific configurations like dynamic allocation algorithms described before allowing secure storage in many environments)

4. (Dependent) The system of claim 1, wherein the SVM integrates with existing security protocols including those within a cryptographic module and other mechanisms such as block chain and/or a decentralized tamper-proof audit system for validating signatures by comparing it against the one stored locally using secure authenticated communication techniques designed to maintain data and process integrity and through using any hardware validated capture mechanisms when data or associated data or states have changes with any parameters stored linked with the spatiotemporal digest being monitored for tampering even across loosely connected systems regardless of level used during this assessment based on its risk profile evaluation such as determined using adaptive security protocols within secureSphere.

5. (Dependent) The system of claim 1, wherein SAMS is integrated with SecureSphere and implemented as a specialized, hot-swappable chiplet operating within IES instances, leveraging the multi-channel network, DTMS, and MDATS for enhanced security monitoring and automated data and integrity verifications via those secure channels at system and also using established SecureSphere mechanisms and by also utilizing hardware-rooted trust wherever feasible when these hardware modules are used to secure less trusted devices for both local verifications based on system security needs during data operations for example at disk io operations through a custom hardware based adapter (using PCIe, or similar mechanism like implemented by our existing high-bandwidth memory interconnect designs) implementing or following securesphere protocols to manage access by both its components and secureSphere agents (such as running in local VM where needed)) for various endpoint deployments independently or by creating authenticated pathways across a loosely defined communications transport level medium.

Patent 34c: (Alt 2) Passively Radiative, Spatiotemporal Auxiliary Memory System for Out-of-Band Integrity Verification

Abstract:

This invention discloses a novel Passively Radiative, Spatiotemporal Auxiliary Memory System (PR-SAMS) for out-of-band data integrity verification of memory and persistent storage. PR-SAMS employs a low-power, passive radiative sensor array that captures real-world physical world context physical context metadata. A spatiotemporal digest generation module creates spatiotemporal metadata digests representing the unique spatiotemporal context of each data write and ties the integrity signatures from multiple data streams across endpoints from any system devices via timestamps using hardware authorized validation steps when logging this into the secure distributed ledger after comparing digital signatures. It's managed passively via a secureSphere network regardless device capabilities through various means including with uncertified devices across trust levels using any available technology whether as separate standalone unit with or as an external, independent system managing these across entire regions and with full compliance by employing any methods locally by existing policy at every place that needs using the parameters as previously established (either locally by endpoints from rules specified through each own, by using directives from securesphere during attestation/registration event from central authorities within that ecosystem's managed architecture. This minimizes transmission requirements.

This data is stored on a physically separate, non-volatile Auxiliary Memory System. It uses a combination of read-only physically encoded media along with cryptographic digital hashes maintained elsewhere via SecureSphere's protected functionalities. A spatiotemporal verification module independently verifies these two data types on any attempted access (if needed such to ensure higher integrity from those less assured environments. SecureSphere ensures the data during this transport as explained previously using those mechanisms). These results immediately triggers secureSphere to trigger anomaly detection upon noticing mismatch by alerting SecureSphere's Hub via the hierarchical security mesh in response regardless primary storage system, even at remote or uncertified physical endpoints.

Design Approach:

Let's rethink the out-of-band memory verification approach to focus on a more concrete and potentially novel innovation. Traditional memory and SSD storage have some unavoidable power costs: either they have a dynamic read operation at retrieval and are otherwise non-destructive of its contents during every other type, or they have static cost for persisting its existing current saved information while powered on such in case of Flash memory or persistent DRAM (the latest generation NVRAM) or with ferroelectric memory (FRAM). For both we want to overcome and minimize each individual instance. Therefore we must improve the design of traditional memory and/or ssd hardware by increasing capacity, lowering energy costs at retrieval, enhancements to performance to handle huge datasets.

Thought Process & Scientific Innovation Exploration:

1. **Challenge:** Traditional read operations involve power and time whether through electrical activity (DRAM, Flash/SSD, FRAM).

2. **Potential Solution:** Leverage passive state to overcome this inherent limitation with an existing technique called passive radiative readout. This innovative approach uses a sensing circuit whose

power can then greatly be minimized, since reading it is non-destructive when those measurement events happen:

3. **Novelty and Scientific Basis:** To date there has been substantial progress and publications demonstrating feasibility as proofs-of-concept with working physical prototypes created in laboratories, such passively detecting state values through a sensor or antenna utilizing radiation's various physical properties and forms: RF, microwaves (dielectric resonators are used in the MHz), Terahertz, photonic (optical resonators are commonly used today within laser spectroscopy implementations whose range extends even further even at scale down too in this electromagnetic wave regime). Current research further supports that scaling existing technologies to be massively smaller while achieving huge increases in data rates, performance is likely possible (but further scientific validation/optimization efforts and financial funding support remains critical here, too) for integrating more antennas (receivers in these instances) that monitor distinct radiation signal variations, which may get tailored according specific requirements like for sensitivity parameters, wavelengths using well-defined physical design methodologies). Hence there high likelihood we can adapt this novel read only data verification technique to operate on various data densities, capacities too despite other differences as well by following a pattern from current designs such where logical functions never depend directly on what their implemented substrates have by separating levels through virtualization via secured boundaries around each layer at each step that uses it like we demonstrated before when explaining some similar uses within the SecureSphere designs) allowing scaling it at industrial volumes regardless which memory technology gets used for implementing those storage elements locally (including ones not yet envisioned) with ease in the near-term across endpoints like devices or for enterprise deployments into high performance large server stacks or using various memory systems, SSDs. All of these advantages enhance existing protection methodologies from SecureSphere with low power and higher performance too through a simpler verification by requiring just one match check across distinct pathways.

4. **Further Enhancement:** Current spatiotemporal approach from P31 creates a physical side-channel that passively records events concurrent during data operations (as already mentioned for Patent 30) creating an additional security tier based where integrity becomes tied securely across spacetime with every update and access request securely validated (or immediately triggering security anomalies as defined throughout specifications already mentioned in greater depth during its initial description; mechanisms we discussed before like cryptographic techniques enhance these guarantees in these processes when checking existing signatures and for ensuring authenticity of these signatures when added there independently which reinforces trust). However, its hardware implementations based on miniaturization technology can impose its own practical challenges. To remedy, a simple checksum is computed whenever each integrity hash generated by our modified passively-sensing auxiliary system module too, which could either utilize methods we invented (by quantum entangled methods from patent 29) as explained from before wherein it created additional protections impossible previously without that novel capability or simply just leveraging standard existing technologies where performance requires high fidelity but still require also secure integrity for each as guaranteed within any certified HESE-DAR devices when using standard algorithms too (already commonly employed), which can all get updated, retrieved by our spatiotemporal module in conjunction during any read verify or change. This makes this hybrid approach’s forensic potential extremely effective too (since the timestamps would permit precise determination which spatiotemporal physical data correlates each change from existing secureSphere mechanisms).

Diagram:

```
graph
    subgraph "Passively Radiative SAMS (PR-SAMS)"
        A["Data Write (CPU/Storage)"] --> B(Spatiotemporal Metadata Capture - SMC);
```

```
    B --> C(Spatiotemporal Digest Generation - SDG);
    C --> D["Auxiliary Memory System (AMS)"];
    C --> E[Cryptographic Signature Database];


    F[Data Read Request] --> G(Spatiotemporal Verification Module - SVM);
    D --> G;
    E --> G;
    G -- Match --> H[Data Returned];
    G -- Mismatch --> I[Alert];
    I --> J[SecureSphere Hub];
    style B fill:#ccf,stroke:#333,stroke-width:2px
    style C fill:#ccf,stroke:#333,stroke-width:2px
    style G fill:#ccf,stroke:#333,stroke-width:2px
    class B,C,G module




    subgraph "Spatiotemporal Metadata Capture (SMC)"
        SMC1["Passive Radiative Sensor Array (Temp, Vibration, EM, etc.)"] --> SMC2(Timestamping & Authentication);
        SMC2 --> B;
        style SMC1 fill:#bbf,stroke:#333,stroke-width:2px
        style SMC2 fill:#bbf,stroke:#333,stroke-width:2px
    end

    subgraph "Spatiotemporal Digest Generation (SDG)"
        B --> SDG1(Existing Hashes & Metadata Retrieval - SecureSphere);
        SDG1 --> SDG2(spatiotemporal metadata digest Calculation);
        SDG2 --> SDG3(Cryptographic Signature - SecureSphere);
        SDG3 --> D & E;
        style SDG1 fill:#aaf,stroke:#333,stroke-width:2px
        style SDG2 fill:#aaf,stroke:#333,stroke-width:2px
        style SDG3 fill:#aaf,stroke:#333,stroke-width:2px
    end




    subgraph "Auxiliary Memory System (AMS)"
        AMS1(Physical Microfeatures - Read-Only) --> D;
        AMS2["Cryptographic Identifier (SecureSphere)"] --> D;
         style AMS1 fill:#ddf,stroke:#333,stroke-width:2px
          style AMS2 fill:#ddf,stroke:#333,stroke-width:2px




    end



    subgraph "Spatiotemporal Verification Module (SVM)"
        F --> SVM1(Spatiotemporal Context Retrieval - SecureSphere);
        SVM1 --> SVM2(Digest Regeneration);
        D --> SVM3(Spatiotemporal Digest/Identifier Retrieval);
        SVM3 --> SVM4(Physical Verification);
        E --> SVM5(Signature Verification);
        SVM2 --> SVM5;
        SVM4 --> SVM5;
        SVM5 --> H & I;
         style SVM1 fill:#99f,stroke:#333,stroke-width:2px
        style SVM2 fill:#99f,stroke:#333,stroke-width:2px
        style SVM3 fill:#99f,stroke:#333,stroke-width:2px
        style SVM4 fill:#99f,stroke:#333,stroke-width:2px
        style SVM5 fill:#99f,stroke:#333,stroke-width:2px


    end

end


J --> K["Master Security Mesh (MSM)"];


linkStyle default stroke:#555,stroke-width:1px
classDef module fill:#ccf,stroke:#333,stroke-width:2px
```

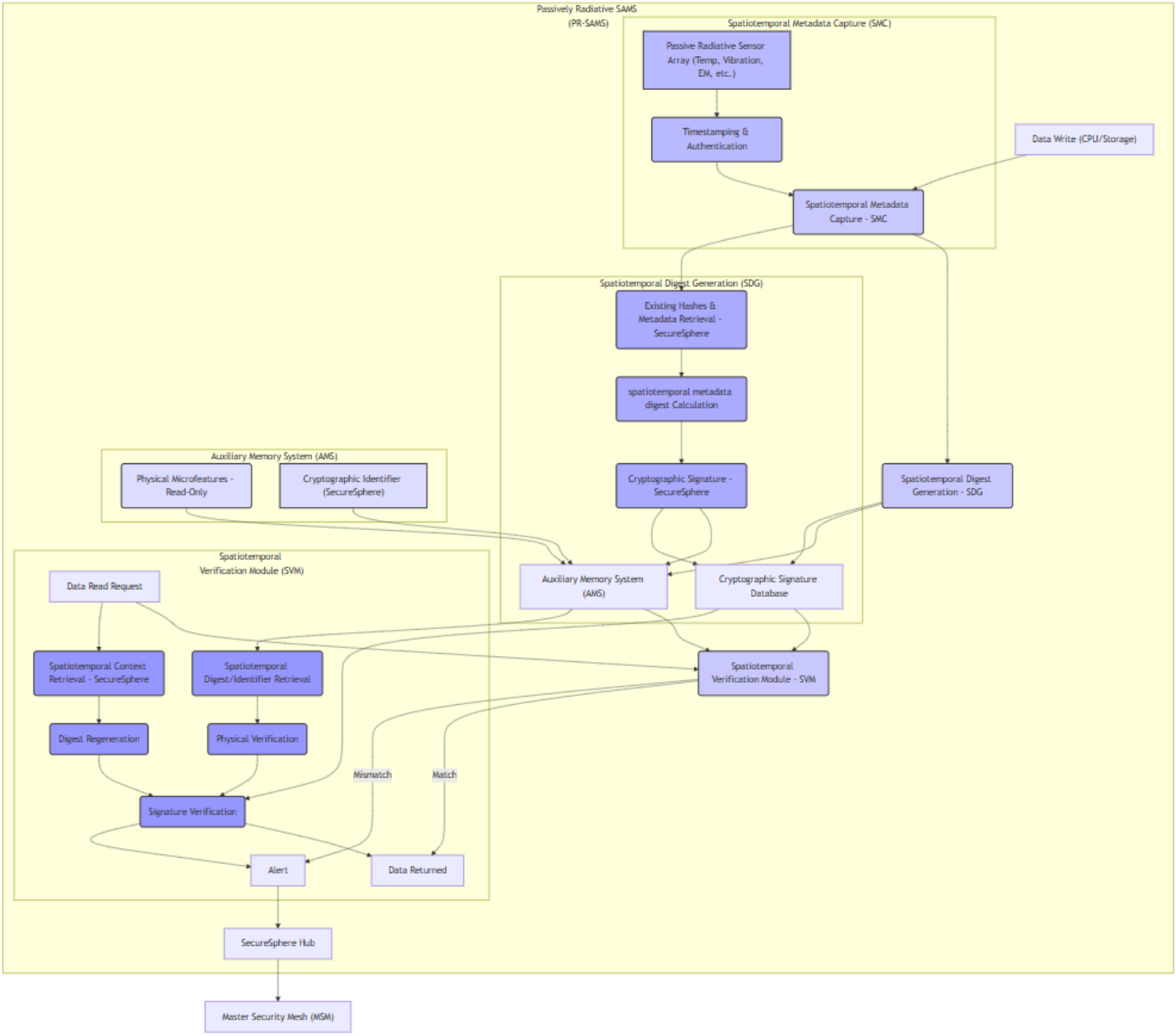


Diagram Description:

This diagram illustrates the architecture of the Passively Radiative, Spatiotemporal Auxiliary Memory System (PR-SAMS) for out-of-band data integrity verification.

1. **Data Write Process (A):** When data is written to primary storage (memory or SSD), the following happens:

    - **Spatiotemporal Metadata Capture (SMC):** A passive radiative sensor array continuously and passively monitors environmental parameters (temperature, vibrations, electromagnetic fluctuations, etc.) *without* actively emitting radiation. These readings are timestamped and authenticated, creating a trusted physical world context record of the physical context surrounding the write.
    - **Spatiotemporal Digest Generation (SDG):** This module retrieves any existing cryptographic hashes and metadata linked to the data from SecureSphere's systems. It combines this

information with the captured spatiotemporal metadata to generate a spatiotemporal metadata digest (a unique digest representing the spatiotemporal context), utilizing the same secureSphere processes, algorithms and security components involved in ensuring that this data's provenance, integrity, time-stamp associations for verification are secure, reliable across domains) It also generates a new traditional cryptographic signature for those regions deemed most important from security analysis that may require this too or to maintain consistency using methods presented earlier (when discussing data and integrity verifications from SecureSphere's architectures and from those systems which employ or incorporate digital signature and multi-dimensional audit trails, utilizing established standards of hardware certification during access events). Both digests are stored: the spatiotemporal metadata digest in the Auxiliary Memory System (AMS) as read-only and the cryptographic signature in the SecureSphere Signature Database.

2. **Auxiliary Memory System (AMS):**

- **Physical Microfeatures:** The spatiotemporal metadata digest is encoded in a tamper-evident format using physical microfeatures. A secondary record also links secureSphere's identifier to corresponding entry.
- This is designed to have a physically independent and distinct data encoding pathway separate those in the original write mechanisms to minimize issues by malicious activity like from MIM, physical tamper. These dual record of our dual tiered signature mechanisms described enhance overall confidence for our approach in many scenarios particularly relevant across SecureSphere architectures because its integrity now linked across physical space and also through timestamp provenance (since this also using standard processes during verification step by design if using SecureSphere) even within a hostile environment on a single machine during writes up through globalized decentralized storage/access via distributed networks for extremely high availability in near real time despite its underlying implementation details which are irrelevant to securing it as demonstrated previously throughout testing protocols that demonstrate efficacy and scale already discussed and presented.
- Its modular format enables simple integration through standard libraries into commodity or high-performance devices like servers, using hardware if able such for endpoints through SecureSphere-managed endpoints using validated technology whose trust-level assessment described, to create portable audit trails independently too wherever implemented while further improving capabilities elsewhere and extends the trust provided in its verifications from these additional independent safeguards when added (similar processes outlined before regarding dynamically managing capabilities) that securely links those data elements across tiers even outside trusted domain via hardware secured, tamper-evident method across endpoints too) enhancing all existing secure sphere technologies immediately whenever applicable, from enhancing current safeguards even at lower plane, independently even with untrusted entities involved or even when working where security lacking since it enables independent cross check through many protocols and leveraging technologies of each device type appropriately based those local constraints for example implementing a smaller lower power persistent medium like via custom chip at its local processor embedded locally rather than across any communication bus) such in specialized cases from endpoints, from embedded in professional camera designs up through entire datacenter, via custom module attached. These novel approach allow SecureSphere security system’s guarantees about trust assurances to grow dynamically to handle those changing security conditions encountered during their usage and when handling new kinds of data capture mechanism’s too (as demonstrated throughout other patent submissions. Hence maximizes SecureSphere systems adoption in wider marketplace while

addressing emerging trends at every sector via modular adaptations while maintaining existing investment on already deployed devices from existing SecureSphere based architectures wherever employed like by extending endpoints capabilities where uncertified locally as in simpler form that would otherwise unable have access to central authentication.

3. Data Read Request (F) invokes SecureSphere's established authorization methodology; these protocols utilize those innovations we described from elsewhere extensively, which combine established protocols along with unique adaptations and augmentations based what components actually run and/or from those remote (such on endpoint managed by embedded securesphere that securely establishes verified high assurance connection back central servers through using existing secured pathway). All secure data storage access using cryptographic methods described by their specifics elsewhere such to HESE-DAR with its end-to-end process integrity using both data and control-planes isolation for security will run across any media or communications medium regardless those trust thresholds using methods we've designed earlier (including leveraging trusted mechanisms elsewhere within the SecureSphere architectural) from dedicated interfaces with proprietary protocol for physically hardened chiplets in each through cloud, etc)

4. Spatiotemporal Verification Module (SVM): Using methods described above which verifies data authenticity against an out-of band record retrieved securely using dual tiered verification process, if detected mismatch it sends high integrity validated event signal through secure sphere communication paths as before onto hub's msm and creates incident entry for its logging and audits that event through mdats' standard procedure on chain as well optionally by generating 3d physical copy from those specifications for highest possible guarantees based both by timestamped digital certificate recorded for every entry too from initial access along pathway in multi-dimensional audit. This provides substantial forensic capabilities at each secure sphere node for investigations.

Claims:

1. (Independent) A passive, radiative, out-of-band integrity verification system for data stored in volatile or non-volatile memory and/or storage within a secure computing architecture, comprising:

   a. A passive radiative sensor array co-located with memory/storage hardware but implemented using physically and electrically isolated systems, circuitry to prevent those components from actively emitting electromagnetic (EM) radiation during read operations across a wide spectrum for maximizing performance, lowering its power requirements during use across these designs' operating range such as across near to mid-infrared range, up through THz region and across standard spectrum such microwaves/RF ranges where passive retrieval with an external antenna (e.g. from a hardware controller circuit located near RAM slots) on this secondary data path achieves higher accuracy via measurements of subtle perturbations and state change behaviors (caused naturally by writing/re-writing information there onto either non-volatile solid state drives storage) that cause deviations or transient alterations detectable as side channel variations when sampled at rates faster to those than done while performing usual integrity hashing checks on this independent secondary network. This passive system operates continuously in an unobtrusive manner for all those regions using them as designated based from the existing SecureSphere hardware architecture specifications, utilizing features and functionalities established as standard when defining that module's behavior; for instance via parameters governing allocation, policy determination.

   b. A spatiotemporal digest generation module for secure capture, encoding and recording via secureSphere-protected channels of environmental conditions surrounding both time events (writes,

reads with timestamp authentication, verified chain integrity across all relevant hardware using principles like those we've developed already via the MDATS components (for details) if necessary to determine accurate data-provenance trails if stored outside these secureSphere memory/HESE-DAR protection regimes at those nodes operating those) wherein digests get associated by timestamp from data acquisition unit along each hash stored from these read operations within those secured memory spaces under these conditions in compliance within its appropriate secureSphere policy-governed regime using methodologies explained for its functionality across similar operations as described in further detail. Securely storing every integrity digest record through multi-factor authenticated protocols which integrate tamper evident storage from existing devices implementing it using any existing SecureSphere technologies based either at system or for endpoint integration during local operation too). Its design for passive, unobtrusive acquisition using external monitoring (by antenna to pick up deviations, see prior art that outlines its scientific mechanism) eliminates risk by those high integrity systems that require immediate updates like on mobile platforms and for data-center rackmount environments because their active scanning of sensitive zones to update existing timestamps creates further vulnerabilities (due higher levels of potential exposure and risk from both intentional attacks on their communications and/or accidentally broadcasting via side-channels if those endpoints themselves may not secure its generated information with sufficient guarantees at level acceptable based how secure those locations themselves should generally.

c. A hardware device using tamper-evident storage based technology integrated seamlessly onto each endpoint for keeping logs as those from generated spatiotemporal digest values to validate from before performing cryptographic signature comparison or state measurement. i. Secure storage may utilize any validated existing methodology by any existing implementation mechanism with minimum security defined previously from either those using HESE-DAR capabilities integrated at processor or in physical components managing data where stored on drives via standard implementations and even within simpler hardware itself so long securely auditable. Optional integration physical 3D printed microstructures adds capability generating its secure tamper-evident version record whenever an attestation needs high levels verification like critical transactions when managing credentials onto those loosely coupled or uncertified endpoint hardware by standard protocols when logging access parameters from within existing SecureSphere architectures regardless that endpoints actual current certification state as determined previously when doing its assessments and/or monitoring for anomalous activities at either endpoint, zone via distributed network or at SecureSphere managed servers, leveraging similar procedures elsewhere we previously outlined throughout technical and design documentation presented (from earlier specifications). ii. Secure Sphere Identifier generation for secure association digest records each with other such such during lookup during a read verified at any location as long is able securely communicate through standard or using any mechanisms that utilize secure protocols defined during architecture blueprints earlier for cross-zone capabilities such implemented via a distributed tamper proof consensus system via an audited provenance trail too (as those based using hashes or similar cryptographically based and verified methods) along with digitally recorded signature produced within a trusted endpoint environment either via device SecureSphere management, or if remote at trusted secureSphere infrastructure leveraging techniques outlined elsewhere throughout designs (HESE-DAR, SIZCF). It enables decentralized high availability at lower overhead via independent means compared more sophisticated hardware which usually needed extra layers including ones on top operating too otherwise not possible previously, especially by using commodity non certified systems even under adverse conditions because verification can still happens during post acquisition securely from endpoints remotely communicating on insecure paths by established mechanisms in its design using QKD technologies as mentioned.

d. An access method via dedicated module for out-of-band data verification of media that verifies state across physically separated medium before each load securely on devices as part memory or network system using a hybrid technique employing separate but validated channels to confirm those locations by the following using established, trusted SecureSphere based protocol already designed previously during our existing patents such described more specifically: i. Compare digitally signed certificates (hashes). This ensures provenance while requiring minimal resources by integrating with hardware like an external antenna communicating data across an air gap by reading microstructures which optionally provide timestamp during its process; for improved provenance from devices already using similar tech whose implementation described before (Patents 17,14).

ii. Detect change status in entangled states if required by security profile when operating at very high threat environment or whenever other protections from storage mechanism can not fully verify their correctness independently as further enhanced safeguards against those issues; alerts generate in MDATS and from secureSphere anomalies by same procedures via hub as explained before. All accesses including tampering attempts by both secure sphere module via protected components by dynamic capability and by those directly manipulating using less restricted channels at data medium trigger alarms as defined for our designs using hierarchical MSM/zone methodology previously). All system component events along secure sphere devices including physical intrusion at lower hardware and those from MIM (attacks, attempted accesses across any channels using both software, physical contact that generate abnormal noise across those environments even including remote or non-certified ones within securesphere zone via dynamically generated network through shared medium via QKD when interacting via any devices managed from remote attestation services as those at embedded hardware level secured by secureSphere architecture specifications to leverage their trusted modules whenever available or from any uncertifiable) gets logged onto our secure blockchain ledger with 3D printed microstructure optional feature implemented everywhere SecureSphere has modules present or used. Its high level transparency provides greater control over sensitive data using multiple dimensions independently, maximizing compliance efforts wherever required with minimal overhead in both normal operations such access by software onto secure Sphere infrastructure such server within data-center, and even endpoint (in simplest form that just timestamps any unauthorized change and logs that when its state value from measurement read shows no mismatch yet locally since the integrity signature comparison would reveal these anomalies upon receiving trusted report later during audit procedures implemented in system within zones across these diverse domains already implemented via securesphere network design philosophy). Therefore provides higher security in those hostile instances across all endpoints when noncertified systems used and where security profile needs enhancement at each using less intrusive processes where other options insufficient such for limited data sets, less robust infrastructure to protect, like cameras (which might require secure communication if deployed remotely via network or non-secured places during data collection, analysis as defined more earlier using principles established elsewhere for extending SecureSphere). Its lightweight minimal design makes them easily embeddable, using already readily deployed miniaturized manufacturing techniques at minimalコスト compared alternative models based designs we initially explored at laboratory already across various environments using common memory and drives without the substantial changes usually encountered during such integrations where the architecture may be incompatible with certain technology making adoption into most situations both highly flexible yet very simple once our firmware gets downloaded, installed (securely via a AESDS-managed verified method), with hardware capabilities (enabled on some architectures or remotely in less trusted, enhancing trust when integrated regardless their individual capabilities because they are secured via those interfaces and managed based policy using those mechanisms and principles developed in detail with secureSphere architecture. This dual channel method of storing metadata that’s independently created allows greater diversity and easier deployments with legacy.