EntangleX: A Quantum-Inspired Cybersecurity System for Post-Breach Data Control

BACKGROUND

Field of the Invention:

The current invention focuses on a cybersecurity solution that facilitates data control after a breach by utilizing entangled copies of data and multi-dimensional vaulting, which enables the real-time oversight and manipulation of data that has been compromised, even if it has already been exfiltrated.

Description of the Related Art:

In the current digital landscape, data has become one of the most prized assets for organizations, making its safeguarding a key strategic focus. As reported by IBM in their 2024 Cost of a Data Breach Report, the average global expense associated with a data breach has increased to $4.88 million, reflecting a 10% rise from the previous year and representing the highest figure on record. This concerning trend highlights the escalating financial, operational, and reputational dangers linked to cyberattacks.

Present-day data protection methods heavily depend on encryption technologies and regular backups. Nonetheless, these strategies are increasingly falling short because of the rapid advancements in technology, particularly the rise of quantum computing. As quantum technology develops, it is anticipated to undermine current encryption methods, placing extensive amounts of sensitive data in jeopardy. However, current technologies offer no effective means to regain control over data once it has been exfiltrated highlighting the urgent need for a post-breach governance mechanism.

SUMMARY

The present invention, EntangleX, introduces a cybersecurity framework that enables persistent data control and sovereignty, even after a breach. Upon detecting unauthorized access, the system triggers a real-time response by extracting the original data from its active environment and securely transferring it to an airgapped vault through a unidirectional hardware bridge or software-controlled data diode, ensuring one-way data flow and preventing external access. The data is then fragmented and distributed across multiple dimensions (spatial, temporal, and computational) thereby increasing isolation and making unauthorized reconstruction significantly more difficult. Simultaneously, the system generates two logically linked data copies: Entangle A, which replaces the original at its location, and Entangle B, which is sent to the unauthorized party. These copies remain synchronized through a logical linkage, enabling any changes made to Entangle A (such as modification, corruption, or deletion) to be mirrored in Entangle B. This architecture establishes a dynamic post-breach governance model, allowing organizations to actively observe, control, or destroy compromised data even

outside their own networks, thereby redefining cybersecurity from passive prevention to active post-intrusion management.

BRIEF DESCRIPTION OF THE DRAWINGS

The following figures provide visual representations of the EntangleX cybersecurity framework and its key operational components, illustrating both the system architecture and its internal logic flow.

FIG.1-System Overview of EntangleX: A high-level diagram depicting the overall data flow of the system, from breach detection to the generation and synchronization of entangled data copies."

FIG.2-Multi-Dimensional Storage and Vaulting : A diagram demonstrating the fragmentation and secure storage of the original data across spatial, temporal, and computational dimensions within an airgapped vault.

FIG.3-Entangled Copy Creation Process: focused illustration of how the system creates Entangle A and Entangle B from the original data, and how a logical entanglement link is established between them.

FIG.4A-Live linkage and control: This figure illustrates the real-time synchronization between Entangle A and Entangle B, showing how any modification to Entangle A is mirrored in Entangle B.

FIG.4B-Example Action: A specific example highlighting how a modification performed on Entangle A results in an immediate mirrored change in Entangle B, demonstrating dynamic post-breach control.

FIG.5-Event Driven Flowchart: A flowchart outlining the operational logic of the EntangleX system, from access monitoring and unauthorized access detection to vaulting, entangled copy creation, synchronization, and post-breach response actions.

DETAILED DESCRIPTION

Upon detection of unauthorized access (10), the EntangleX system begins by extracting the original data (12) from its active location as in FIG.1.

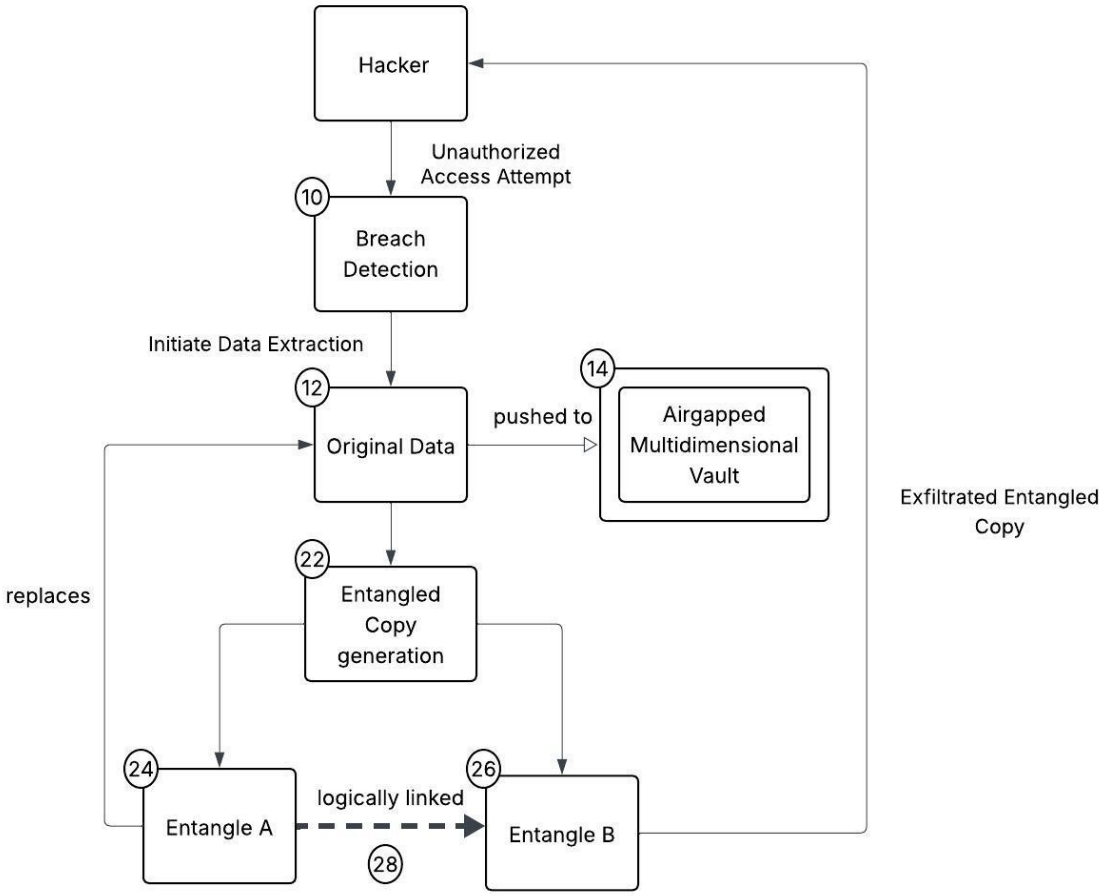

FIG.1: System Overview of EntangleX

This data is securely transmitted via a one-way mechanism to a multidimensional airgapped vault (14), where it is fragmented and stored in isolated temporal (16), spatial (18), and computational (20) dimensions as in FIG.2. Temporal fragmentation may involve tiered retention schedules or version-based isolation to allow rollback and targeted deletion over time. Spatial fragmentation may include dispersal across geographically distributed storage nodes or containerized vaults with region-specific access policies. Computational fragmentation applies differing encryption standards, access protocols, or algorithmic filters based on resource context, making reconstruction of the complete dataset computationally prohibitive.

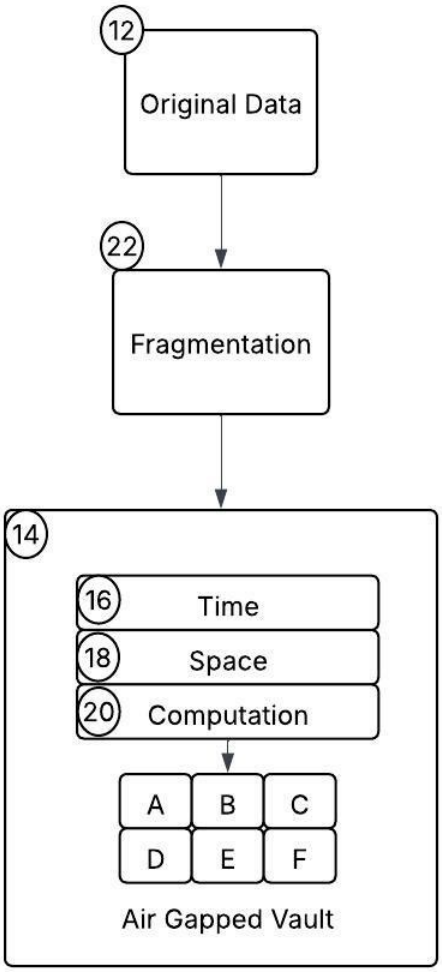

FIG2: Multi-Dimensional Storage and Vaulting

Simultaneously, the system generates two logically linked data copies (22): Entangle A (24), which replaces the original data at the original location, and Entangle B (26), which is exfiltrated to the unauthorized user as shown in FIG.3. A logical entanglement link (28) is established between two instances Entangle A and Entangle B via a secured synchronization engine that continuously monitors Entangle A and unidirectionally mirrors corresponding state or content-level modifications onto Entangle B. Entangle B operates in a passive, non-authoritative mode, disallowing local modifications or upstream interactions. The synchronization linkage may leverage mechanisms such as checksum verification, time-stamped state differencing, or encrypted, unidirectional triggers, each governed by controlled propagation policies to ensure integrity and secure, source-bound data flow as shown in Fig3.

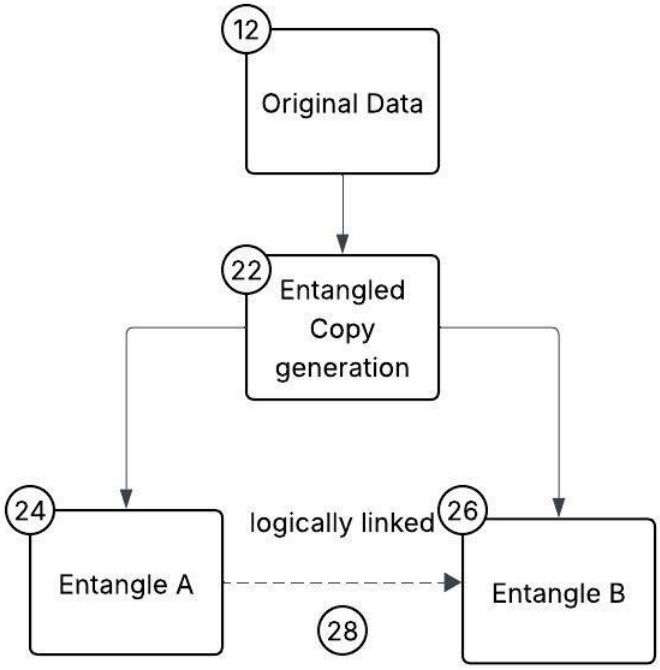

FIG.3: Entangled Copy Creation Process

Modifications to Entangle A (30) are mirrored in Entangle B (32) shown in FIG.4b, enabling real-time control, deception, or neutralization of the attacker's copy.

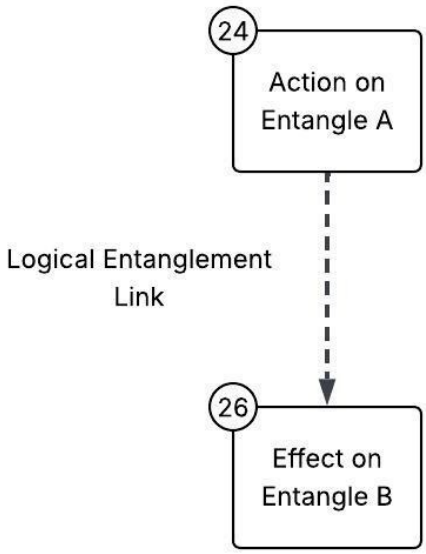

FIG.4A:Live linkage and control

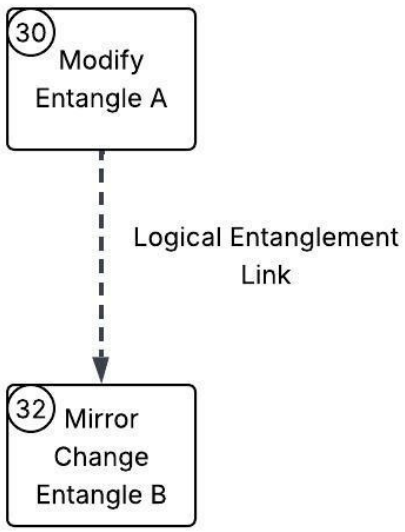

FIG.4B:Example Action

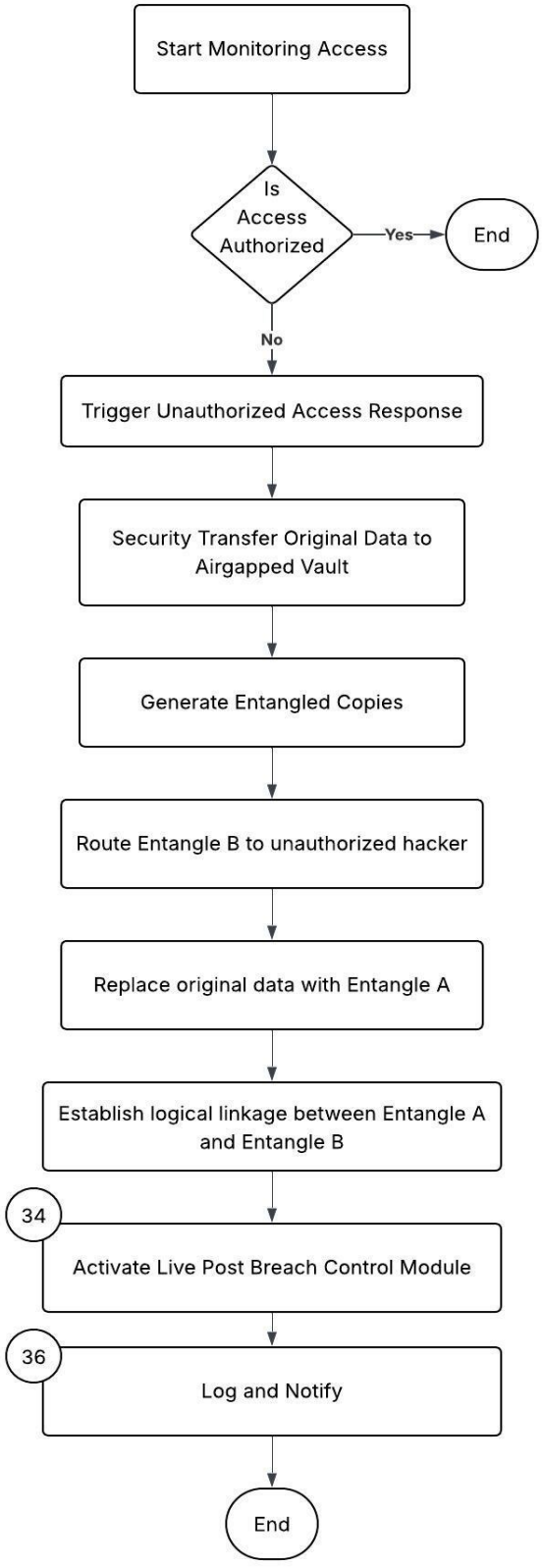

FIG5: Event-Driven Flowchart

The EntangleX system also includes a live post-breach control console (34) that allows authorized users to manage Entangle A and, by extension, Entangle B. Actions taken via this console are logged (36) and reported to designated incident response personnel for auditing and compliance as shown in FIG.5.

Preferred Embodiment:
The favored implementation of this invention employs a one-way data diode to guarantee secure conveyance to the vault, along with containerized storage distributed between cloud and local segments for multidimensional protection. The fragmentation logic is supported by AI to dynamically adjust encryption keys and access requirements.

Alternate Embodiments:
Other embodiments may include hardware vaults, zero-knowledge proof access control, or integration with blockchain for immutable audit trails.

Quantum-Inspired Design Intent:
While the current implementation uses logical synchronization to establish entanglement between data copies, the architecture is designed to support future integration of quantum mechanisms. These may include quantum key distribution, quantum-based entanglement systems, or quantum communication protocols. The behavior of Entangle A and Entangle B is inspired by quantum entanglement in that any change to one is reflected in the other, regardless of location. This conceptually mirrors the non-local correlation seen in quantum systems and sets the foundation for a future quantum-enhanced version of EntangleX.

CLAIMS

1. A method for controlling data after a breach, comprising: detecting unauthorized access to digital information; retrieving the digital information from its original location; transferring the retrieved digital information to a protected, multidimensional vault; generating a primary data copy, referred to as Entangle A, to replace the original data at its location, and a secondary data copy, referred to as Entangle B, for delivery to an unauthorized user; and establishing a logical synchronization link between Entangle A and Entangle B, such that any changes made to Entangle A are unidirectionally reflected in Entangle B.

2. The method of claim 1, wherein the step of transferring the extracted digital data to the secure, multidimensional vault is performed via a unidirectional data transfer mechanism.

3. The method of claim 2, wherein the spatially isolated storage nodes utilize independent access control policies, the temporally partitioned storage utilizes varying data retention schedules, and the computationally isolated storage utilizes distinct encryption schemes.

4. The method of claim 1, the extracted digital data is transmitted using a unidirectional data transfer mechanism to a secure multidimensional vault designed to block any reverse data flow.

5.A system for post-breach data control, comprising a breach detection module configured to detect unauthorized access to digital data; a vaulting mechanism configured to securely store extracted digital data in a multidimensional vault; an entangled copy generation module configured to generate a first data copy (Entangle A) and a second data copy (Entangle B); a synchronization module configured to unidirectionally mirror modifications from the first data copy to the second data copy through a logical link; and a control interface configured to allow authorized users to modify the first data copy.

6.The system of claim 5, wherein the multidimensional vault comprises storage distributed across at least two of the following: spatially isolated storage nodes, temporally partitioned storage, and computationally isolated storage.

7.The system of claim 6, wherein the spatially isolated storage nodes implement independent access controls; the temporally partitioned storage applies varying retention policies; and the computationally isolated storage utilizes differing encryption keys.

8.The system of claim 5, further comprising a unidirectional data transfer mechanism configured to transfer the extracted digital data to the vaulting mechanism.

9.The system of claim 5, wherein Entangle B is rendered immutable and read-only, and the logical link prohibits direct updates to Entangle B from any source other than Entangle A.

10.A framework for data governance following a cybersecurity breach, largely as outlined here with reference to the illustrations and specific embodiments.

ABSTRACT

EntangleX is a groundbreaking cybersecurity solution inspired by quantum principles, designed to provide persistent control over digital information even after a breach occurs. Upon detecting unauthorized access, the system instantly creates two entangled data copies, one sent to the infiltrator (Entangle B), and the other retained securely (Entangle A). Simultaneously, the original data is removed from its active location, pushed into a multi-dimensional airgapped vault, and replaced by Entangle A in its original spot. This architecture enables real-time alteration, corruption, or destruction of the stolen copy, ensuring post-breach data sovereignty and dynamic defensive control.

Signature: Sunil Kumar Peela
Date: 4/23/2025
Location: Fort Collins, Colorado, USA