HORIZON EUROPE

Research and Innovation Actions (RIA)

Proposal Part B - Technical Description

SYNAPSE

Next-Generation Distributed Neural Architectures for Privacy-Preserving Collaborative AI

Topic:	HORIZON-CL4-2026-HUMAN-01-02 – Collaborative Edge AI
Type of Action:	Research and Innovation Action (RIA)
Project Duration:	36 Months
Total Budget:	EUR 4,850,200
Coordinator:	Synapse Research Institute (France)

List of Participants

No.	Participant Organisation Name	Country	Role
1	Synapse Research Institute (Coordinator)	France	CO
2	Nexa Autonomous Systems	Germany	BEN
3	Vertex Advanced Laboratories	Italy	BEN
4	Nimbus Technologies	Spain	BEN
5	Meridian Systems Group	Sweden	BEN

Contents

1 Excellence **3**

1.1 Objectives and Ambition . . . 3

1.2 Methodology . . . 3

1.2.1 Overview of the Technical Pipeline . . . 3

1.2.2 Scientific Quality and Ambition . . . 3

2 Impact **4**

2.1 Project's Pathways towards Impact . . . 4

2.2 Measures to Maximise Impact: Dissemination and Exploitation . . . 4

3 Quality and Efficiency of the Implementation **4**

3.1 Work Plan and Resources . . . 4

3.2 Critical Risks for Implementation . . . 4

1 Excellence

1.1 Objectives and Ambition

The primary objective of the SYNAPSE project is to develop and validate a decentralized, privacy-preserving AI framework that allows heterogeneous edge devices to collaboratively train deep learning models without transferring raw data. By establishing secure, high-efficiency computation paradigms, SYNAPSE addresses the fundamental trade-offs between privacy, accuracy, and network consumption in edge ecosystems.

Project Vision

SYNAPSE envisions a future where intelligent systems learn collectively while guaranteeing absolute local data sovereignty. Our methodology bridges the gap between privacy-preserving technologies (homomorphic encryption, differential privacy) and energy-constrained edge deployment.

We define three specific, measurable, and realistic objectives (Table 1) to guide the research and technical development over the 36-month timeline:

Table 1: Specific Project Objectives

Objective	Description	Key Performance Indicator
Obj 1	Develop robust decentralised aggregation algorithms resilient to noisy client updates.	Standard convergence rate within 5% of centralised baselines.
Obj 2	Integrate hardware-accelerated homomorphic encryption for low-power edge chips.	Execution overhead less than 1.5x relative to unencrypted runs.
Obj 3	Validate the SYNAPSE platform in two industrial validation pilots.	Deployment on 50+ heterogeneous nodes in active operations.

1.2 Methodology

The SYNAPSE methodology integrates advanced cryptographic schemes with dynamic network topographies. We move beyond traditional federated learning paradigms by introducing peer-to-peer validation blocks.

1.2.1 Overview of the Technical Pipeline

Our architecture is split into three functional layers: the Edge Execution Layer, the Secure Verification Layer, and the Adaptive Consensus Layer. Figure 1 illustrates the workflow across these modules:

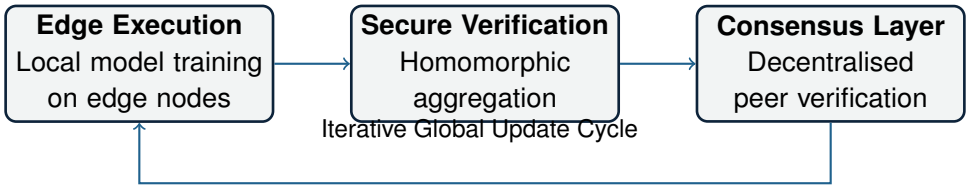

Figure 1: The SYNAPSE dynamic methodology workflow showing iterative decentralized loops.

1.2.2 Scientific Quality and Ambition

The current state-of-the-art (SOTA) in collaborative AI relies on central orchestrators, introducing a single point of failure and systemic privacy vulnerabilities. SYNAPSE bypasses this by introducing a decentralized consensus mechanism based on zero-knowledge proofs. Our mathematical model enforces constraint validation prior to any global aggregation, ensuring that malicious updates are filtered out.

2 Impact

2.1 Project's Pathways towards Impact

The SYNAPSE project is designed to deliver significant impacts across three main dimensions: scientific, technological, and societal. Table 2 highlights these pathways.

Table 2: Project Pathways to Impact

Impact Dimension	Project Pathway	Target Destination
Impact 1: Scientific	Open-source publication of core mathematical proofs and performance benchmarks.	Academic journals, standard repositories (e.g., Zenith-AI archive).
Impact 2: Tech	Standardization of APIs for hardware-agnostic edge crypto-acceleration.	Contribution to IEEE and W3C working groups on decentralized AI.
Impact 3: Social	Enhanced trust in public digital infrastructure through provable privacy guarantees.	Deployment in public services, regional healthcare databases.

2.2 Measures to Maximise Impact: Dissemination and Exploitation

To ensure the long-term sustainability of the project results, the consortium has established a structured plan for dissemination, exploitation, and communication:

- **Exploitation:** Nexa and Nimbus will commercialize the security layer as a software development kit (SDK) for IoT manufacturers, accelerating the adoption of secure edge nodes.
- **Dissemination:** Academic partners (Synapse Research Institute, Vertex) will publish a minimum of 8 peer-reviewed open-access articles.
- **Communication:** Joint workshops, standardization briefings, and a dedicated project website hosted by Meridian Systems.

3 Quality and Efficiency of the Implementation

3.1 Work Plan and Resources

The work plan is structured into five Work Packages (WPs) aligning research, development, validation, and project management tasks:

[WP1] WP1: Coordination and Ethics (Synapse)

[WP2] WP2: Privacy-Preserving Cryptographic Core (Vertex)

[WP3] WP3: Decentralized Architecture and Orchestration (Nexa)

[WP4] WP4: Pilot Integration and Demonstration (Nimbus)

[WP5] WP5: Dissemination, Exploitation and Exploitation Strategy (Meridian)

Table 3 shows the detailed structure of WP2, demonstrating the allocation of tasks and partner resources.

3.2 Critical Risks for Implementation

We have identified prospective technical and operational risks to project execution, accompanied by practical mitigation strategies (Table 4).

Table 3: WP2: Privacy-Preserving Cryptographic Core

Work Package Number	WP2
Lead Participant	Vertex Advanced Laboratories (Italy)
Start Month – End Month	M06 – M24
Person-Months	Vertex: 18, Synapse: 12, Nexa: 6, Nimbus: 4, Meridian: 2
Objectives	Design homomorphic encryption templates for edge accelerators and implement low-latency differential privacy perturbations for local weights.
Description of Work	**Task 2.1: Crypto Acceleration (Vertex, Nexa)** – Adapting lattice-based mathematical schemes to ARM-NEON instructions. **Task 2.2: Noise Calibration (Synapse, Vertex)** – Creating dynamic differential privacy parameter estimation based on node density.
Deliverables	D2.1: Mathematical specifications document (M12) D2.2: Cryptographic core implementation code (M18)

Table 4: Critical Risks and Mitigation Strategies

Risk Description	WP	Likelihood	Proposed Mitigation Strategy
Performance degradation on resource-constrained devices.	WP2, WP3	Medium	Fall back to semi-homomorphic encryption schemes and utilize quantized model parameters.
Interoperability issues between edge architectures.	WP3, WP4	Low	Enforce strict API protocols using standardized containerized environments.
High node dropout rate in pilot scenarios.	WP4	High	Implement asynchronous aggregation models that handle variable dropouts.