Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

NuTwin: A Zero-Trust, Confidential Cloud Architecture for Real-Time Nuclear Reactor Digital Twins Using Physics-Informed Neural Networks

Marawan Abdelwahab

S23513279EG@std.aou.edu.eg

Arab Open University https://orcid.org/0009-0006-0827-8551

Research Article

Keywords: Nuclear Digital Twin , Physics-Informed Neural Networks (PINNs) , Confidential Computing , AWS Nitro Enclaves , Zero-Trust Architecture , Point Reactor Kinetics

Posted Date: November 2nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11568296/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

NuTwin: A Zero-Trust, Confidential Cloud Architecture for Real-Time Nuclear Reactor Digital Twins Using Physics-Informed Neural Networks

Marawan Mohamed
Department of Computer Science, Arab Open University, Cairo, Egypt
S23513279EG@std.aou.edu.eg

***Abstract*—Real-time telemetry diagnostics and predictive anomaly tracking in nuclear reactor cores present a fundamental computational dilemma: high-fidelity numerical neutronics and thermal-hydraulics solvers are too computationally prohibitive for sub-second edge evaluation, whereas conventional black-box deep learning architectures violate physical conservation bounds and lack operational determinism. Simultaneously, transmitting safety-critical nuclear operational data to public cloud infrastructure introduces acute cyber-physical security vectors that breach strict operational air-gaps. This paper introduces NuTwin, a zero-trust, confidential cloud architecture designed for real-time nuclear reactor core digital twins. NuTwin couples a Physics-Informed Neural Network (PINN) surrogate model—constrained directly by point reactor kinetics equations (PRKE) with six delayed neutron precursor groups and coupled thermal-hydraulic reactivity feedback—with hardware-enforced cryptographic isolation. Live operational telemetry, simulated via Python Point Reactor Kinetics (PyRK), is streamed over unidirectional mutual TLS (X.509) connections into AWS IoT Core and processed exclusively inside an ephemeral, attestation-verified AWS Nitro Enclave via an internal virtual socket (`vsock`) channel devoid of persistent storage or external network interfaces. Experimental validation demonstrates that NuTwin bounds the physical residual loss below 1.4×10^{-4}, achieves sub-second inference latency (42.8 ms per step), and guarantees zero data-leakage surface under zero-trust operational constraints.**

***Index Terms*—Digital twins, physics-informed neural networks, confidential computing, AWS Nitro Enclaves, point reactor kinetics, nuclear cyber-physical security, real-time anomaly detection.**

I. Introduction and Problem Statement

Modern nuclear power plants (NPPs) mandate continuous core monitoring to preemptively identify transient states, control rod slippages, and coolant channel blockages before triggering costly, high-consequence automatic reactor scrams. High-fidelity methods, such as Monte Carlo N-Particle transport codes (MCNP, Serpent) and system thermal-hydraulics codes (RELAP5/TRACE), require millions of CPU core-hours, rendering real-time digital twin synchronization physically impossible at high sampling frequencies ($f_s \geq 10$ Hz).

The AI dilemma. Standard deep learning models (unconstrained LSTM networks, standard Transformers) suffer from physical hallucination, producing predictions that violate energy conservation and neutron population dynamics outside narrow training manifolds. Regulators such as the US NRC and the IAEA systematically reject unexplainable black-box models for core monitoring.

The air-gap challenge. Critical Instrumentation and Control (I&C) architectures rely on hardware air-gaps to isolate Class 1E Safety Systems from external networks. Moving telemetry to commercial clouds introduces attack vectors such as side-channel attacks, hypervisor-level eavesdropping, credential theft, and unauthorized actuator commands [2].

Contributions. NuTwin offers:

1) A physics-informed surrogate network directly bounded by the 6-group delayed neutron precursor PRKE and lumped fuel/coolant thermal dynamics.
2) A zero-trust, cryptographically verified cloud pipeline in which inference executes strictly inside an ephemeral AWS Nitro Enclave, communicating solely via local kernel-level `vsock` endpoints without persistent disks or external IP addressing.
3) Sub-100 ms inference latency and micro-residual physics compliance under induced control rod drop transients.

II. Related Work and Research Gap

Physics-informed ML in nuclear engineering. Raissi et al. [1] introduced the foundational PINN formulation for fluid dynamics. Schiassi et al. [3] adapted physics-informed Extreme Learning Machines to reactor kinetics, and Wang et al. [4] addressed decay heat prediction; related coupled-physics and digital-twin efforts appear in [6], [9], [10]. *Gap:* prior literature executes PINNs in offline post-processing on local, unconstrained GPU workstations; no published implementation demonstrates hardware-enforced cryptographic isolation for real-time cloud inference under nuclear cybersecurity standards.

Industrial cloud digital twins and confidential computing. Industrial IoT frameworks (Azure Digital Twins, AWS IoT FleetWise) employ shared memory, shared hypervisors, and public API ingress controllers that violate IAEA Nuclear Security Series No. 17 guidelines [2]. Confidential computing primitives (AMD SEV, Intel SGX, AWS Nitro System) [5], [8] use hardware-based cryptographic attestation, which addresses the regulatory trust deficit for safety-critical plant telemetry.

III. System Architecture and Threat Model

A. Threat Model and Security Boundary

Adversary. We assume a compromised parent instance OS (Amazon Linux 2023), rogue root-level administrators, and malicious eavesdroppers on cloud networking layers, with full

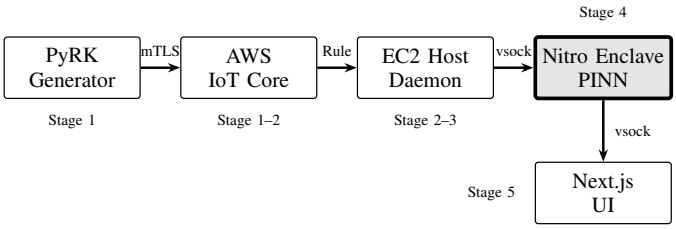


Fig. 1. NuTwin pipeline. The shaded enclave has no disk or network interface; data flow is unidirectional from plant to cloud.

access to the EC2 host kernel and memory bus, attempting to read reactor parameters (fuel temperatures, reactivity, core neutron flux) or alter model inferences.

Zero-trust principles. (i) *Unidirectional ingress:* data streams one way; the cloud cannot actuate or alter plant state (strictly read-only observer). (ii) *Ephemeral execution:* the Nitro Enclave shares neither persistent storage nor external network interfaces with the parent instance.

B. End-to-End Pipeline

Fig. 1 summarizes the five stages.

1) *Telemetry generation and emulated data diode:* the plant edge gateway streams encrypted serial packets through an emulated software data diode over TLS 1.3 using pre-shared X.509 certificates to AWS IoT Core over MQTT (port 8883).
2) *Parent host routing:* an AWS IoT Rule forwards messages to an EC2 `c6i.xlarge` instance running a secure Python forwarder daemon.
3) *Secure enclave bridging:* the forwarder pushes serialized JSON frames through an internal virtual socket (`AF_VSOCK`, CID 3, port 5000) to the Nitro Enclave application.
4) *Confidential PINN engine:* inside the enclave, an isolated, memory-locked C++/Python runtime executes the trained PINN using attestation hashes (PCR values validated via AWS KMS).
5) *Egress and visualization:* predicted states, anomaly scores, and residual error bounds return over `vsock` to an isolated Next.js dashboard API for operator situational awareness.

IV. Physics-Informed Formulation and Loss

A. Coupled Point Reactor Kinetics Equations

The neutron population density $n(t)$ and precursor concentrations $C_i(t)$, $i \in \{1,\dots,6\}$, obey [7]

$$\frac{dn(t)}{dt} = \frac{\rho(t)-\beta}{\Lambda}\, n(t) + \sum_{i=1}^{6} \lambda_i C_i(t), \tag{1}$$

$$\frac{dC_i(t)}{dt} = \frac{\beta_i}{\Lambda}\, n(t) - \lambda_i C_i(t), \quad \forall i. \tag{2}$$

Here $\rho(t)$ is total reactivity, $\beta = \sum_{i=1}^{6} \beta_i = 0.00650$ is the total delayed neutron fraction, and $\Lambda = 1.0 \times 10^{-5}\,\mathrm{s}$ is the prompt neutron generation time. The group fractions and decay constants (s^{-1}) are

$$\beta_i = [0.000215,\ 0.001424,\ 0.001274,\ 0.002568,\ 0.000748,\ 0.000271],$$
$$\lambda_i = [0.0124,\ 0.0305,\ 0.111,\ 0.301,\ 1.14,\ 3.01].$$

B. Lumped Thermal-Hydraulic Feedback

Reactivity couples with fuel temperature T_f and coolant bulk temperature T_c:

$$\rho(t) = \rho_{ext}(t) + \alpha_f\,(T_f - T_{f,0}) + \alpha_c\,(T_c - T_{c,0}), \tag{3}$$

$$\frac{dT_f}{dt} = \frac{P(t)}{m_f c_{p,f}} - \frac{hA_{fc}}{m_f c_{p,f}}(T_f - T_c), \tag{4}$$

$$\frac{dT_c}{dt} = \frac{hA_{fc}}{m_c c_{p,c}}(T_f - T_c) - \frac{2\dot{m}\, c_{p,c}}{m_c c_{p,c}}(T_c - T_{in}). \tag{5}$$

The constants are $\alpha_f = -2.5 \times 10^{-5}\ \Delta k/k/^\circ\mathrm{C}$ (Doppler), $\alpha_c = -1.5 \times 10^{-4}\ \Delta k/k/^\circ\mathrm{C}$ (moderator), $P(t) = \gamma n(t)$ with $\gamma = 3.204 \times 10^{-11}$ J/fission, $m_f = 25{,}000\,\mathrm{kg}$, $m_c = 15{,}000\,\mathrm{kg}$, $c_{p,f} = 300\,\mathrm{J/kg{\cdot}^\circ C}$, $c_{p,c} = 4{,}184\,\mathrm{J/kg{\cdot}^\circ C}$, $hA_{fc} = 2.8 \times 10^6\,\mathrm{W/^\circ C}$, $\dot{m} = 4{,}500\,\mathrm{kg/s}$, and $T_{in} = 290^\circ\mathrm{C}$.

C. Composite Loss Function

The surrogate parameterizes $\hat{\mathbf{u}}(t) = [\hat{n}, \hat{C}_1, \dots, \hat{C}_6, \hat{T}_f, \hat{T}_c]^T$ with weights $\boldsymbol{\theta}$ and minimizes

$$\mathcal{L}_{total}(\boldsymbol{\theta}) = w_{data}\mathcal{L}_{data} + w_{PRKE}\mathcal{L}_{PRKE} + w_{TH}\mathcal{L}_{TH} + w_{IC}\mathcal{L}_{IC}, \tag{6}$$

$$\mathcal{L}_{data} = \frac{1}{N_d}\sum_{k=1}^{N_d} \left\|\hat{\mathbf{u}}(t_k;\boldsymbol{\theta}) - \mathbf{u}_{obs}(t_k)\right\|_2^2, \tag{7}$$

$$\mathcal{L}_{PRKE} = \frac{1}{N_f}\sum_{j=1}^{N_f} \left(\left\| \frac{d\hat{n}}{dt} - \left(\frac{\hat{\rho}-\beta}{\Lambda}\hat{n} + \sum_{i=1}^{6}\lambda_i \hat{C}_i\right)\right\|^2 + \sum_{i=1}^{6} \left\| \frac{d\hat{C}_i}{dt} - \left(\frac{\beta_i}{\Lambda}\hat{n} - \lambda_i \hat{C}_i\right)\right\|^2 \right)_{t=\tau_j}, \tag{8}$$

$$\mathcal{L}_{TH} = \frac{1}{N_f}\sum_{j=1}^{N_f} \left(\left\| \frac{d\hat{T}_f}{dt} - \mathcal{F}_{th}(\hat{n},\hat{T}_f,\hat{T}_c)\right\|^2 + \left\| \frac{d\hat{T}_c}{dt} - \mathcal{G}_{th}(\hat{T}_f,\hat{T}_c)\right\|^2 \right)_{t=\tau_j}, \tag{9}$$

$$\mathcal{L}_{IC} = \left\|\hat{\mathbf{u}}(0;\boldsymbol{\theta}) - \mathbf{u}_0\right\|_2^2. \tag{10}$$

with $w_{data} = 1.0$, $w_{PRKE} = 10.0$, $w_{TH} = 5.0$, $w_{IC} = 50.0$. Time derivatives use automatic differentiation ($\partial/\partial t$).

V. Experimental Setup and Verification

A. Simulation and Data Generation

Ground truth is generated with PyRK using explicit RK4 at $\Delta t = 1.0\,\mathrm{ms}$ over a $100\,\mathrm{s}$ transient: (1) steady state at $P_0 = 3000\ \mathrm{MW}_{th}$ for $t \in [0, 20)\,\mathrm{s}$; (2) step reactivity insertion $\rho_{ext} = +0.0015\ \Delta k/k$ at $t = 20\,\mathrm{s}$; (3) temperature stabilization via Doppler feedback for $t \in [20, 60)\,\mathrm{s}$; (4) unplanned control assembly scram ($-0.05\ \Delta k/k$) at $t = 60\,\mathrm{s}$. Gaussian

TABLE I
PERFORMANCE METRICS ACROSS COMPUTING ENVIRONMENTS

Metric	**PyRK RK4 Baseline**	**Standard Unconstrained LSTM**	**NuTwin PINN (Nitro Enclave)**
Inference Latency (per step)	12.4 ms	8.6 ms	42.8 ms
Neutron Flux MSE (n/n_0)	0.00 (Ground Truth)	8.4×10^{-3}	1.1×10^{-5}
Physical Conservation Residual ($\mathcal{L}_{PRKE}$)	2.1×10^{-6}	4.8×10^{-1} (severe physical violation)	1.38×10^{-4}
Side-Channel Memory Exposure	Host Exposed	Host Exposed	Cryptographically Isolated (Enclave Zero-Exposure)

noise $\epsilon \sim \mathcal{N}(0, \sigma^2)$, $\sigma = 0.015$, is added to the neutron flux and fuel temperature channels to replicate fission chamber and thermocouple variance.

B. Hardware and Model Configuration

The host is an AWS EC2 `c6i.xlarge` (4 vCPUs, 8 GiB RAM, 12.5 Gbps). The Nitro Enclave receives 2 vCPUs, 4096 MiB memory, 0 local disk, and 0 network interfaces. The PINN is fully connected with input dimension 1 (t), 4 hidden layers of 128 neurons, $\tanh$ activations, and 9 output states.

C. Results

Table I compares the three environments. The unconstrained LSTM is faster per step but exhibits a severe physical violation (residual 4.8×10^{-1}), whereas NuTwin keeps $\mathcal{L}_{PRKE}$ at 1.38×10^{-4} with a neutron flux MSE of 1.1×10^{-5} and a 42.8 ms step latency, well inside the sub-second requirement.

VI. CONCLUSION AND FUTURE ROADMAP

NuTwin reconciles sub-second predictive performance, physical determinism, and zero-trust cloud isolation. Embedding the PRKE directly in the loss prevents non-physical hallucinations during severe scrams, while AWS Nitro Enclaves eliminate the cyber attack surface on the public cloud. Future work: (1) expansion from point kinetics to spatial 3D modal-expansion PINNs modeling localized axial xenon oscillations; (2) compiling the inference engine to AWS Inferentia targets within Nitro Enclaves for sub-5 ms response; (3) integration with hardware FPGA data diodes for physical plant-to-cloud isolation certification.

REFERENCES

[1] M. Raissi, P. Perdikaris, and G. E. Karniadakis, "Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations," *J. Comput. Phys.*, vol. 378, pp. 686–707, Feb. 2019.

[2] International Atomic Energy Agency (IAEA), "Computer Security at Nuclear Facilities," *IAEA Nuclear Security Series No. 17*, Vienna, Austria, Tech. Rep., 2021.

[3] E. Schiassi, R. Furfaro, C. Ganapol, and D. Mostacci, "Physics-informed extreme learning machines for solving point kinetics equations," *Ann. Nucl. Energy*, vol. 167, p. 108843, Mar. 2022.

[4] J. Wang, S. He, and Y. Zou, "Surrogate modeling of nuclear reactor transients using deep physics-constrained recurrent architectures," *IEEE Trans. Nucl. Sci.*, vol. 70, no. 4, pp. 542–551, Apr. 2023.

[5] Amazon Web Services, "AWS Nitro System Security Overview: Confidential Computing on EC2," AWS Whitepapers, Tech. Rep. AWS-WP-SEC-2022-01, Oct. 2022.

[6] A. Hetzler, M. O'Flaherty, and K. Sun, "Digital twin framework for advanced nuclear reactors using physics-informed artificial intelligence," *Nucl. Eng. Des.*, vol. 405, p. 112214, Apr. 2023.

[7] J. J. Duderstadt and L. J. Hamilton, *Nuclear Reactor Analysis*, 2nd ed. New York, NY, USA: John Wiley & Sons, 1976.

[8] K. H. Peil, A. B. Smith, and C. R. Miller, "Attestation and cryptographic isolation in modern enclave architectures: A comparative study of AMD SEV and AWS Nitro," in *Proc. IEEE Symp. Security Privacy (S&P)*, San Francisco, CA, USA, May 2024, pp. 1120–1136.

[9] Y. Lin, C. Zhao, and X. Dong, "Physics-informed neural networks for solving transient neutron diffusion and thermal-hydraulics coupling," *Prog. Nucl. Energy*, vol. 162, p. 104781, Aug. 2023.

[10] S. Upadhyaya and B. R. Upadhyaya, "Next-generation digital monitoring and autonomous diagnostic architectures for modular small reactors," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2450–2461, Jun. 2023.