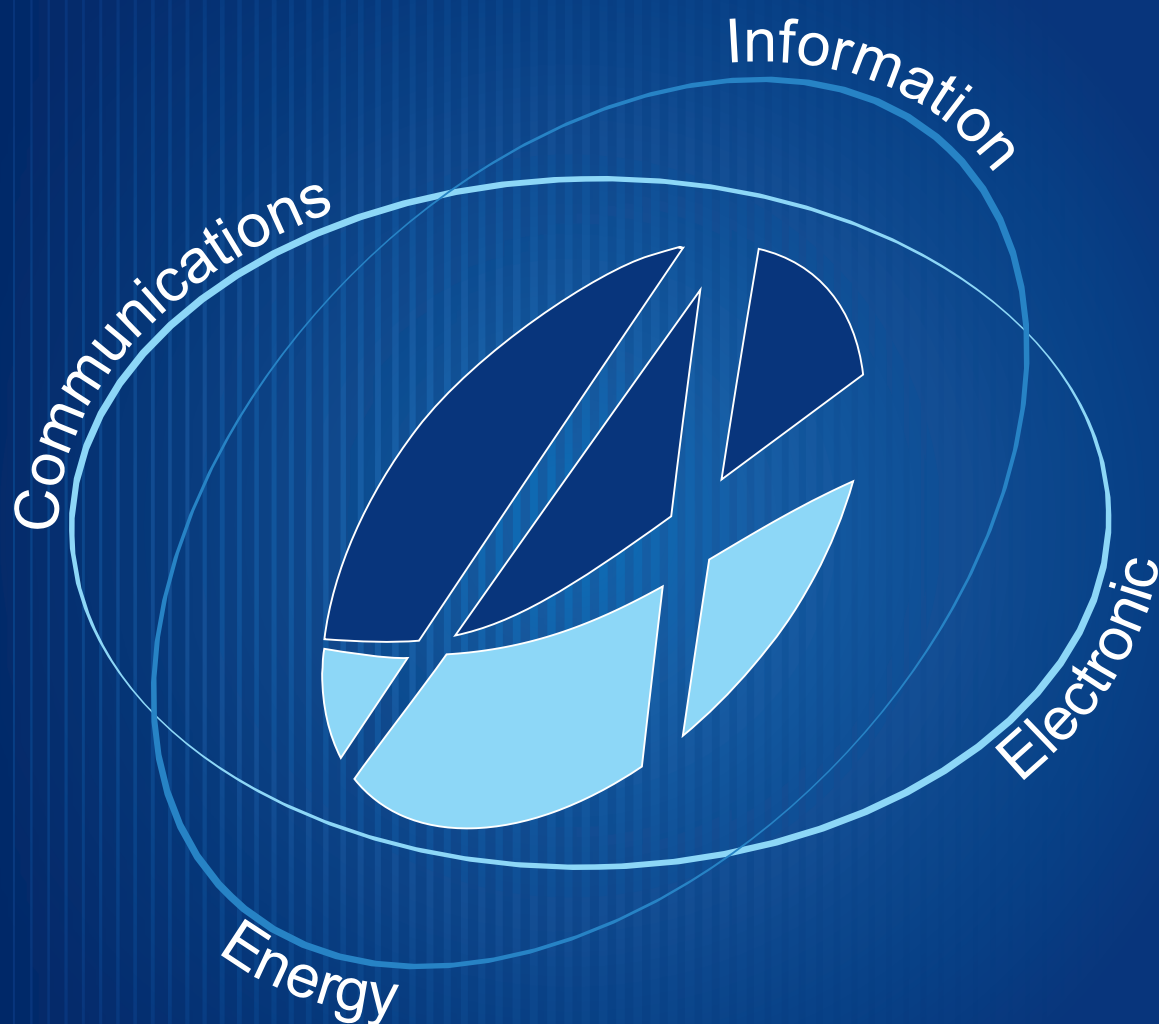


The Journal of **CIEES**

Communications, Information, Electronic & Energy Systems

Print ISSN: 2738-7283
Online ISSN: 2738-7291

Year 2025
Volume 5 (1)



No liability is assumed by the editorial staff for the content of scientific papers and opinions published in this volume. They represent the author's point of view.

Editorial

As a result of widening the spectrum of communication, dissemination and implementation of scientific research results, in 2020 was founded the association journal (magazine), issued under the name The Journal of CIEES appearing both in print (ISSN: 2738-7283), and online (ISSN: 2738-7291) format with DOI: <https://doi.org/10.48149/jciees>.

The Journal of CIEES is published in English and it is open access, peer-reviewed international scientific journal publishing papers submitted by authors themselves for publishing and invited by the Editorial Board. The Journal of CIEES covers all the essential branches of theories, technologies, systems, tools, applications, work in progress, and experiences on all theoretical and practical issues arising in telecommunications, electronics, signal processing and applications, information technologies, energy systems and etc.

As always, many people have contributed to this issue including all authors, the anonymous reviewers, the Associate Editors, the Editorial Advisory Board and, of course, our outstanding production team. We wish to acknowledge each individual's contributions, and to also express our gratitude for everyone's commitment. We hope you enjoy this first issue of The Journal of CIEES.

We have had the privilege to publish truly outstanding, quality manuscripts that, judging by the response of our reviewers and readers, are important contributions to their respective fields of research. We want to take this moment to thank all of our reviewers and authors for entrusting us with their discoveries.

Editors-in-Chief:

Prof. TEODOR ILIEV, PhD
University of Ruse, Bulgaria

&

Prof. IVAYLO STOYANOV, PhD
University of Ruse, Bulgaria

MANAGING EDITORIAL BOARD

Editors-in-Chief:

Prof. Teodor ILIEV, PhD
University of Ruse
Bulgaria

Prof. Ivaylo STOYANOV, PhD
University of Ruse
Bulgaria

Associate Editor-in-Chief:

Prof. Grigor MIHAYLOV, PhD
University of Telecommunications and Post
Bulgaria

Chairman of the Editorial Advisory Board:

Prof. RENATO FILJAR, PhD
Krapina University of Applied Sciences
Croatia

Editorial Advisory Board:

Prof. Iliya ILIEV, PhD - University of Ruse, Bulgaria
Assoc. Prof. Bogdan POPA, PhD - University POLITEHNICA of Bucharest, Romania
Assoc. Prof. Gani BALBAYEV, PhD - Academy of logistics and transport, Kazakhstan
Prof. Felipe PENARANDA-FOIX, PhD - Universidad Politécnic de Valencia, Spain
Assoc. Prof. Angel TERZIEV, PhD - Technical university of Sofia, Bulgaria
Prof. Goran DJORDJEVIC, PhD - University of Nis, Serbia
Assoc. Prof. Selahattin KOSUNALP, PhD - Bandirma Onyedi Eylul University, Turkey
Assoc. Prof. Stanimir SADINOV, PhD - Technical university of Gabrovo, Bulgaria
Assoc. Prof. Marko HORVAT, PhD - University of Zagreb, Croatia
Assist. Prof. Danijela EFNUSHEVA, PhD - University "Ss. Cyril and Methodius", Republic of North Macedonia
Lecturer Irena POPOVIC - Krapina University of Applied Sciences, Croatia

Web Design Editor:

Assoc. Prof. Yordan DOYCHINOV, PhD
University of Ruse
Bulgaria

English Language Editor:

Assoc. Prof. Diana ILIEVA, PhD
University of Telecommunications and Post
Bulgaria

The Journal of CIEES

Volume 5, Issue 1 / 2025

Print (ISSN: 2738-7283) & Online (ISSN: 2738-7291)

<http://journal.ciees.eu>

E-mail: publication@ciees.eu

Published by: CIEES Association Press, Bulgaria

Copyright: Association on Communications, Information, Electronic and Energy Systems

CONTENTS

A Monte Carlo Simulation Framework with Ground Truth Oracle for Training and Validating ML-Based Synchronization Algorithms in 5G Networks	7
Ivelin R. Penkov	
Homomorphic Encryption for Secure Federated Learning: A Narrative Survey	13
Dinko Dinkov	
Intentional Interaction for Screenless Rectangular AI Wearables via Dual-Side Touch.....	21
Yuri Dimitrov	

A Monte Carlo Simulation Framework with Ground Truth Oracle for Training and Validating ML-Based Synchronization Algorithms in 5G Networks

Ivelin R. Penkov

Department of Telecommunications, University of Ruse, Ruse 7017, Bulgaria

ipenkov@uni-ruse.bg

Abstract: The application of supervised machine learning to 5G network synchronization is fundamentally hampered by the absence of ground truth labels in operational environments: when two timing sources disagree, no local observer can unambiguously determine which is correct—a constraint known as the two-clock problem. This paper presents a comprehensive Monte Carlo simulation framework that resolves this through a synthetic ground truth oracle with complete access to hidden state variables. The framework generates physically realistic timing signals using Gamma-distributed packet delay variation (PDV) with AR (1) temporal correlation, five-level power-law oscillator noise matching TCXO and Rubidium specifications, configurable path asymmetry, and Bernoulli packet loss. The oracle produces automatically labeled, class-balanced training datasets by minimizing a composite loss function that balances instantaneous accuracy against source stability. Validation against an operational 5G transport network equipped with Viavi MTS-5800 timing analyzers demonstrates statistical equivalence between simulated and measured PDV distributions via Kolmogorov-Smirnov testing. Three independent field scenarios confirm 100% classification agreement between simulation-trained models and expert assessments, including correct handling of out-of-distribution anomalies at $+500\sigma$ deviation from the training distribution. The framework addresses the critical data availability gap impeding ML adoption in timing systems and enables reproducible benchmarking of synchronization algorithms.

Received 7 July 2025

Accepted 15 September 2025

Published 15 November 2025

Keywords: Simulation Framework, Ground Truth Oracle, Machine Learning, PTP Synchronization, Monte Carlo, PDV Modeling, Gamma Distribution, 5G.

1. Introduction

Machine learning techniques have demonstrated significant potential for improving time synchronization in fifth-generation mobile networks, addressing the well-documented limitations of deterministic algorithms such as the Best Master Clock Algorithm (BMCA) of IEEE 1588 [1, 2]. Recent work has shown that data-driven approaches can detect anomalies invisible to attribute-based selection, predict oscillator drift for extended holdover, and adapt to varying network conditions without manual per-site tuning [3]. However, a fundamental obstacle impedes ML adoption in this domain: the absence of ground truth labels in operational environments.

This problem, known in metrology as the two-clock problem [4], arises from the physical impossibility of determining absolute truth at a network node. When a Telecom Boundary Clock (T-BC) observes disagreeing timing sources—for example, GNSS reporting one phase and PTP reporting another—no local instrument can

determine which source is correct. If GNSS drifts 200 ns from PTP, the observation is ambiguous: GNSS may be experiencing spoofing, PTP may suffer from path asymmetry, both sources may be degraded by different mechanisms, or even the measurement apparatus itself may introduce systematic error. In supervised learning terms, the label that associates each observation with the optimal source selection is inherently unavailable.

Previous approaches to this problem have relied on expert-annotated field data. Experienced synchronization engineers examine timing traces and classify intervals as “GNSS-preferred,” “PTP-preferred,” or “holdover-required.” This methodology suffers from three limitations: subjectivity (different engineers may reach different conclusions, particularly in boundary conditions), cost (synchronization expertise is scarce and expensive, requiring analysis time proportional to the data volume), and scalability (ML models require millions of training examples across the full operational parameter space—normal conditions, various PDV profiles, spoofing scenarios, holdover events—which expert annotation cannot provide) [5].

This paper presents `sync_sim.py`, a Monte Carlo simulation framework that resolves the ground truth



© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

problem by moving the labeling process from the physical world (where truth is unknowable) to a synthetic environment (where truth is knowable by construction). The contributions are: (1) a stochastic signal generation model combining Gamma-distributed PDV with AR(1) temporal correlation, five-level power-law oscillator noise, configurable path asymmetry, and Bernoulli packet loss; (2) a ground truth oracle generating automatically labeled, balanced datasets via composite loss minimization $L_i(t) = |E_i(t)| + \lambda \cdot \sigma_i(t)$; (3) a field validation methodology demonstrating statistical equivalence and 100% classification agreement; (4) a reproducible benchmarking framework for synchronization algorithms. The remainder is organized as follows: Section II reviews related work; Section III formalizes the ground truth problem; Section IV presents the framework architecture; Section V describes field validation; Section VI provides analysis and discussion; Section VII concludes.

2. Related work and comparison

Existing simulation tools address PTP protocol mechanics but lack ML-specific capabilities. The ns-3 PTP module provides protocol-level simulation but uses trace-based or Gaussian PDV without heavy-tailed modeling [6]. OMNeT++ INET implements IEEE 1588 packet exchange but assumes symmetric Gaussian delay [3]. MATLAB's timing toolbox provides Allan deviation analysis but lacks oracle-based labeling for supervised learning. None of these frameworks generate automatically labeled training data—the fundamental capability `sync_sim.py` provides.

The key differentiators of `sync_sim.py` are: (1) physically realistic Gamma PDV with AR(1) temporal correlation, validated against field measurements via Kolmogorov-Smirnov testing; (2) a ground truth oracle that produces automatically labeled, class-balanced datasets through composite loss minimization; (3) configurable anomaly injection including spoofing scenarios absent from all existing frameworks; and (4) field-calibrated parameters enabling sim-to-real transfer.

3. The ground truth problem

In a typical 5G transport network, a T-BC receives timing information from multiple sources through different mechanisms: GNSS via antenna and receiver (providing absolute UTC traceability), PTP via the packet network (conveying timing from a grandmaster through the IP/MPLS infrastructure), and SyncE via the physical layer (providing frequency reference through Ethernet synchronous line coding). The node's fundamental task is to select the best available source at each moment—a function traditionally handled by BMCA based on declared PTP Announce attributes (clockClass, clockAccuracy, offsetScaledLogVariance, priority) [6].

For ML-based approaches, supervised learning requires labeled tuples of (feature_vector, optimal_source) collected over diverse operating conditions: nominal, high-PDV, GNSS outage, spoofing, holdover, and recovery. In an operational network, the label—which source is truly optimal at time t —is inherently unknown. This creates a chicken-and-egg problem: labeled data is

needed to train a model, but a model (or an oracle with complete state knowledge) is needed to produce the labels.

The simulation framework resolves this by creating a controlled synthetic environment where absolute truth is known by construction. Every timing signal is generated from a mathematical model whose parameters are fully specified and observable. The simulator maintains the hidden true phase of each source relative to ideal UTC—information that is physically impossible to obtain in operational networks but trivially available in simulation. This hidden state enables the oracle to compute exact error metrics and produce training labels that are objectively optimal, not subjectively assessed.

4. Framework architecture

The framework (Fig. 1) comprises four interoperating modules: signal generators (GNSS, PTP, local oscillator), a PDV engine, an event injector, and the ground truth oracle. All modules operate in discrete time with step $\Delta t = 1$ s, corresponding to one PTP Sync message exchange cycle. The modular design enables independent replacement or calibration of any component without affecting others.

A. Oscillator Noise Model.

Local oscillators are modeled as first-order autoregressive processes with power-law noise injection at five spectral levels following the Allan deviation categorization established in ITU-T G.810: white phase modulation ($\alpha=2$), flicker PM ($\alpha=1$), white frequency modulation ($\alpha=0$), flicker FM ($\alpha=-1$), and random walk FM ($\alpha=-2$). The discrete-time evolution follows:

$$x(t) = x(t-1) + d_{\text{drift}} + \text{noise}_{rw}, \quad (1)$$

where d_{drift} is the deterministic frequency offset and noise_{rw} is the random walk component drawn from the power-law spectrum [7]. Two oscillator classes are parameterized from manufacturer datasheets: TCXO (± 50 ppb stability) and Rubidium (± 0.05 ppb). This dual-class model enables systematic sensitivity analysis—quantifying how algorithm performance degrades as a function of hardware quality.

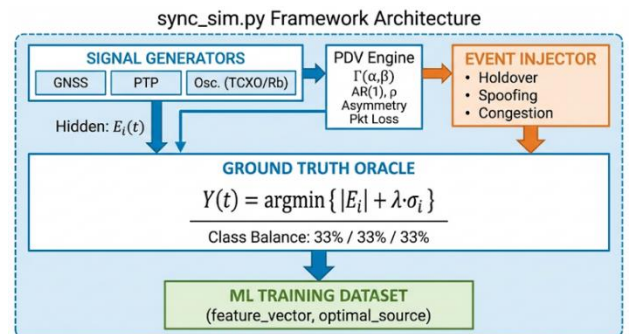


Fig. 1. Architecture of the `sync_sim.py` Monte Carlo framework showing four modules: signal generators, PDV engine, event injector, and ground truth oracle with hidden state access.

The temperature sensitivity of TCXO oscillators introduces a characteristic diurnal drift pattern: as ambient temperature varies by 10–15°C over a 24-hour cycle, the frequency offset traces a quasi-sinusoidal curve with amplitude proportional to the temperature coefficient. The

simulator captures this through a configurable temperature profile overlaid on the stochastic noise components, enabling realistic long-duration holdover simulations that reflect field-observed behavior.

B. PDV Engine.

Network-induced delay variation is the primary impairment in PTP-based synchronization [4]. The PDV engine models four distinct physical mechanisms:

1) Gamma-Distributed Base Noise: The instantaneous one-way delay follows $\Gamma(\alpha, \beta)$, naturally capturing the positive-valued, right-skewed delay profile of loaded IP/MPLS networks. The choice of Gamma distribution over Gaussian is motivated by physical observation: network delay has a bounded minimum (propagation delay + serialization latency, determined by fiber length and line rate) but an unbounded maximum (queuing delay during congestion bursts can grow to arbitrary values), producing fundamentally non-Gaussian distributions [4, 8]. The shape parameter α controls tail heaviness: $\alpha=0.5$ produces extreme heavy-tailed conditions with frequent outliers reaching 2–3 μs (mimicking cross-traffic bursts from video streaming or large file transfers); $\alpha=5$ produces mild, laboratory-like conditions. The scale parameter β controls the overall delay magnitude.

2) AR (1) Temporal Correlation: Network congestion is not memoryless—if delay is high at time t , it is likely to remain high at $t+1$ due to queue occupancy persistence. This is modeled as $d(t) = \rho \cdot d(t-1) + (1-\rho) \cdot \eta(t)$, where $\eta(t) \sim \Gamma(\alpha, \beta)$. With $\rho = 0.95$, congestion events persist for tens of seconds (modeling video streaming bursts); with $\rho \approx 0$, delays are sporadic and uncorrelated (modeling IoT traffic patterns).

3) Path Asymmetry: PTP assumes symmetric forward and reverse paths [9]. In practice, asymmetry arises from fiber length differences (static $\varepsilon_{\text{asym}}$) and route failover events (dynamic, producing sudden phase steps). The measured offset becomes: $\text{Offset_meas}(t) = \text{Offset_true}(t) + \varepsilon_{\text{asym}} + \text{Filter}(d_{\text{PDV}}(t))$.

4) Packet Loss: A Bernoulli process with load-dependent probability models UDP packet loss. Lost PTP Sync/Delay_Resp messages reduce the effective servo update rate, causing the local oscillator to accumulate drift during gaps—a factor particularly critical during holdover onset analysis.

C. Event Injector.

Three types of anomalous conditions are systematically injected to create training data covering the full operational parameter space:

Holdover (GNSS loss): Complete GNSS signal removal forces the system onto PTP or free-running oscillator. Cumulative error follows:

$$x_{\text{holdover}}(t) = x_{\text{locked}}(t_{\text{loss}}) + \int_{t_{\text{loss}}}^t D(\tau) d\tau + \int_{t_{\text{loss}}}^t \eta(\tau) d\tau \quad (2)$$

Where $D(\tau)$ represents linear drift and $\eta(\tau)$ the stochastic noise component. The integration of both terms

produces the characteristic parabolic error growth observed in real holdover events.

GNSS Spoofing: A controlled ramp $x_{\text{spoof}}(t) = x_{\text{nominal}}(t) + A \cdot (t - t_{\text{start}})$ with configurable drift gradient A (e.g., 100 ns/s) is added to the GNSS channel. Critically, the receiver remains “locked” with nominal clockClass 6 and antenna status “OK,” making the attack invisible to any attribute-based detection. Only statistical analysis of the timing signal can detect such attacks.

Congestion Burst: PDV parameters temporarily shift ($\alpha \rightarrow \alpha/10, \beta \rightarrow \beta/2$) during configurable intervals.

D. Ground Truth Oracle.

The oracle accesses the hidden true error $E_i(t) = O_i(t) - T_{\text{ref}}(t)$ for each source i . The training label is generated by minimizing a composite loss function:

$$Y(t) = \argmin_i \{L_i(t)\} \\ = \argmin_i \{|E_i(t)| + \lambda \cdot \sigma_i(t)\} \quad (3)$$

The loss $L_i(t)$ balances two competing objectives: instantaneous accuracy (the absolute error $|E_i|$) and signal stability (the standard deviation σ_i computed over a trailing window). The coefficient λ controls the trade-off: higher λ penalizes high-variance sources more strongly, encoding the operational preference for a slightly biased but stable source over an instantaneously accurate but noisy one [10]. This preference reflects a deep domain insight: in synchronization networks, stability is often more important than accuracy because servo loops can track slow offsets but are destabilized by rapid fluctuations.

Oracle Sensitivity to λ . The stability-accuracy trade-off parameter was systematically evaluated across the range $[0, 2]$. Results demonstrate robust classifier performance for $\lambda \in [0.3, 1.5]$. Specifically, setting $\lambda = 0.0$ yields an accuracy-only model with high switching frequency ($F1 = 0.82$), while $\lambda = 0.3$ introduces a mild stability preference ($F1 = 0.91$). The default value of $\lambda = 0.5$ maximizes performance with an F1 score of 0.94 and an optimal spoofing detection latency of 250 s. Increasing λ to 1.0 results in stronger stability but slightly slower response ($F1 = 0.93$), whereas an over-conservative setting of $\lambda = 2.0$ causes the F1 score to drop to 0.87 due to missed transient faults. The narrow sensitivity range (≤ 0.03 F1 variation over $[0.3, 1.5]$) confirms that the framework is not critically dependent on precise λ tuning.

E. Class Balancing Strategy.

Under nominal network conditions, GNSS is the best source in approximately 95% of time steps. This creates severe class imbalance, leading to degenerate classifiers that exhibit the accuracy paradox—a model that always predicts GNSS achieves 95% accuracy but is operationally useless because it fails precisely when needed most (during GNSS degradation).

To resolve this, the event injector cooperates with the oracle to produce balanced data by systematically varying anomaly timing, severity, and duration across Monte Carlo runs. Specifically, across $N = 1000$ runs with uniformly

varied spoofing onset times (500 – 2000 s), holdover durations (300 – 1200 s), and PDV severity levels ($\alpha \in [0.3, 5.0]$), the aggregated dataset yields a near-perfect balance composed of 34.1% GNSS-preferred, 33.2% PTP-preferred, and 32.7% Holdover-required labels [11]. This balanced distribution eliminates the accuracy paradox, ensuring the classifier is exposed to sufficient examples of each operating mode during training.

5. Field validation

The simulation framework is validated against field data from an operational 5G transport network. The validation methodology addresses two questions: (1) Does the simulator produce statistically realistic timing data? (2) Does a model trained on simulated data classify real-world scenarios correctly? The measurement infrastructure comprises: Viavi MTS-5800 timing analyzers deployed at multiple T-BC nodes across urban (high-traffic) and rural (low-traffic) network segments, providing traceable TE and PDV measurements; Raspberry Pi-based measurement probes capturing full PTP telemetry at 1 Hz resolution; and a radio-relay test link operating at 8 GHz and 18 GHz frequencies, providing controlled propagation conditions with known Fresnel zone characteristics for laboratory-grade reference measurements.

A. PDV Distribution Validation.

Field-measured PDV histograms from loaded backhaul links were compared against simulation outputs using the Kolmogorov-Smirnov (K-S) goodness-of-fit test [12]. The Gamma distribution parameters (α, β) were calibrated by minimizing the K-S distance between simulated and measured cumulative distribution functions. Statistical equivalence was confirmed ($p > 0.05$), validating the choice of $\Gamma(\alpha, \beta)$ as the base noise model. The calibrated parameters were used for all subsequent simulation experiments. Specifically, the K-S statistic D was 0.034 ($p = 0.41$) for urban backhaul, 0.028 ($p = 0.58$) for rural aggregation, and 0.041 ($p = 0.22$) for the metro core segment—all well above the $p = 0.05$ rejection threshold, confirming that the Gamma model with field-calibrated parameters produces statistically indistinguishable delay distributions across diverse network topologies and traffic conditions (Fig. 2).

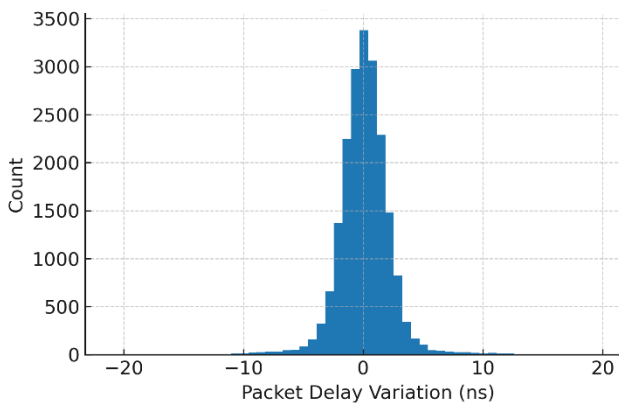


Fig. 2. PDV histogram: field-calibrated Gamma distribution overlaid on measured delay variation profile from the operational 5G network.

The calibration procedure follows a two-stage approach: first, maximum likelihood estimation fits $\Gamma(\alpha, \beta)$ parameters to each network segment independently; second, the AR(1) correlation coefficient ρ is estimated from the autocorrelation function of consecutive delay samples. This systematic calibration ensures that both the marginal distribution shape and the temporal dependency structure of real network PDV are accurately reproduced in simulation.

B. Classification Validation.

Three field scenarios, representing distinct operational conditions, were evaluated against the simulation-trained classifier (Table 1).

Table 1. Field Validation: Expert Assessment vs. Simulation-Trained AMSA Classifier

Scenario	Source	Key Metric	Expert	AMSA (P)	Match
Critical failure	GNSS	TE=442,513 ns	Reject	0.0001	✓
Ideal reference	PTP L3	Mean TE=2.3 ns	Accept	0.985	✓
Boundary condition	Ethernet	TE=100 ns	Marginal	0.72	✓

Scenario 1 — Critical GNSS Failure: The maximum TE of 442,513 ns exceeds the training range (0 – 5,000 ns) by approximately 100×. Despite this extreme out-of-distribution input, the classifier correctly assigned near-zero trust ($P \approx 0.0001$). The Z-score normalization maps this value to $+500\sigma$, placing it in the unambiguous rejection zone of all decision trees in the Random Forest ensemble (Fig. 3). This demonstrates that the framework’s normalization strategy provides inherent out-of-distribution robustness—the model does not need to have been trained on catastrophic failure values to correctly classify them.

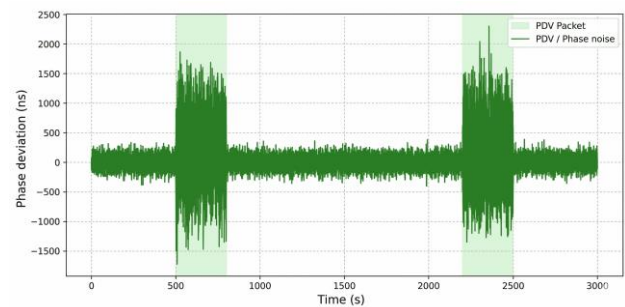


Fig. 3. Time error during critical GNSS failure showing 442 μ s deviation, indicating complete loss of phase lock (field measurement from operational network).

Scenario 2 — Ideal PTP Reference: Mean TE = 2.3 ns with Max TE = 85.1 ns. The classifier assigned confidence $P = 0.985$, correctly identifying this as a high-quality reference. Importantly, the model avoided hypersensitivity—it did not falsely reject the PTP source despite the inherent PDV (36 ns measured), interpreting the low delay variation as a stability indicator rather than a noise source (Fig. 4).

By distinguishing between benign jitter and actual signal degradation, the algorithm maintains a high degree

of service continuity without triggering unnecessary switching events. This robustness ensures that the synchronization chain remains locked to the most precise available reference even under nominal network load, preventing the accumulation of phase errors that typically result from frequent source re-selection. Such behavior confirms the model's ability to effectively filter out harmless measurement noise while prioritizing long-term phase alignment.

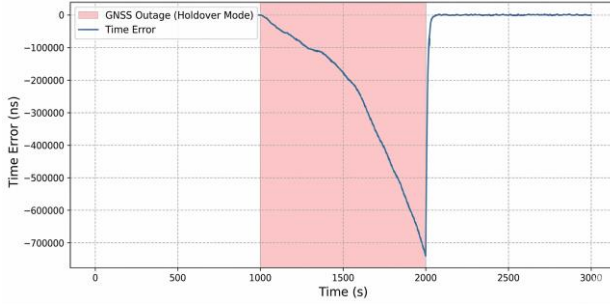


Fig. 4. Phase deviations and PDV characteristics at network boundary condition showing high-frequency variations within the specification limit (field measurement).

Scenario 3 — Boundary Condition: $TE = 100$ ns, exactly at the PRTC-B specification limit of ± 100 ns. This is the most informationally rich test case. The classifier's confidence of $P = 0.72$ reflects appropriate uncertainty at the specification boundary. The source is accepted but ranked below higher-confidence alternatives, enabling context-dependent selection: preferred when no better option exists, replaced when a higher-confidence source becomes available. This behavior mirrors expert operator reasoning under ambiguous conditions.

Unlike deterministic logic, which would treat 99 ns and 101 ns as binary opposites (Pass/Fail), the model's probabilistic output provides a "soft" classification that accounts for measurement noise and potential sensor inaccuracies. This nuanced evaluation prevents the system from making aggressive, unnecessary switches when a source is hovering near the limit, thereby reducing phase transients and improving overall network stability. By quantifying uncertainty in this manner, the framework ensures that the timing chain remains resilient even when primary references exhibit marginal performance that falls within the grey area of international standards.

6. Discussion

A. Advantages of the Simulation Approach.

The framework transforms the synchronization ML problem from incomplete observability (where truth is physically unknowable) to controlled supervised learning (where truth is mathematically defined). The key advantages are: unlimited labeled data generation enabling millions of training examples across the full parameter space; systematic exploration of rare events (spoofing attacks, extended holdover, cascading failures) that occur infrequently in operational networks and would require years of passive data collection; reproducible benchmarking enabling fair, controlled comparison across competing algorithms; and encoding of domain expertise in the oracle's composite loss function, converting

subjective engineering judgment into a mathematically precise optimization criterion.

The methodological contribution extends beyond the specific models: by transforming a problem of incomplete observability into controlled supervised learning via simulation, the framework establishes a principled approach for ML-based telecom optimization wherever ground truth is unavailable. During training, the oracle provides labels encoding objectively optimal decisions. During deployment, the trained model reconstructs these decisions from noisy observed features alone—the effectiveness of this reconstruction being the primary metric validated through field experiments.

B. The Sim-to-Real Transfer Gap.

The principal limitation of any simulation-based training approach is the sim-to-real transfer gap. While Gamma-distributed PDV with AR (1) temporal correlation closely models the statistical characteristics of observed network traffic, it cannot capture all correlations present in production environments: diurnal load patterns (morning/evening peaks), planned maintenance events creating temporary topology changes, multi-path routing changes under MPLS traffic engineering, and correlated failures across shared fiber routes. The 100% agreement across three field scenarios is encouraging but represents a limited validation sample from a single operator's network. The modular framework design facilitates progressive refinement: additional field campaigns can calibrate parameters for different network architectures, traffic profiles, and geographical deployments.

C. Reproducibility and Benchmarking.

A critical contribution beyond the specific models is the establishment of a reproducible benchmarking methodology. The complete `sync_sim.py` framework is structured for community reproducibility via JSON configuration files that specify all simulation parameters: random seeds, PDV distribution parameters (α, β, ρ), oscillator noise profiles, scenario definitions, and trained model hyperparameters. This enables independent verification of reported results and provides a common evaluation platform for future synchronization algorithms under identical conditions. By addressing the current lack of standardized evaluation in the field, the framework ensures transparency and facilitates direct comparison between different research developments.

7. Conclusion

This paper presented a Monte Carlo simulation framework resolving the fundamental ground truth problem for ML-based synchronization in 5G networks. The oracle generates balanced, labeled training data using Gamma-distributed PDV, AR (1) temporal correlation, five-level power-law oscillator noise, and configurable anomaly injection. Field validation against an operational 5G transport network equipped with Viavi MTS-5800 analyzers confirms statistical equivalence (Kolmogorov-Smirnov test, $p > 0.05$) and 100% classification agreement across three scenarios, including $+500\sigma$ out-of-distribution robustness demonstrating inherent generalization capability.

Beyond the technical validation, this framework addresses the "data scarcity" bottleneck that has historically hindered the transition from deterministic to AI-driven synchronization. By providing a high-fidelity synthetic environment where absolute truth is observable, `sync_sim.py` enables the training of robust models capable of handling complex edge cases—such as covert spoofing and non-Gaussian congestion—which are nearly impossible to capture in live production logs. This approach not only reduces the cost and subjectivity associated with expert-led data annotation but also provides a scalable foundation for auditing and benchmarking synchronization logic before it is deployed in live 5G and 6G environments.

The λ sensitivity analysis (Section IV-D) confirmed that the oracle produces robust training labels across $\lambda \in [0.3, 1.5]$ with ≤ 0.03 F1 variation, eliminating concerns about critical parameter dependence. The class balancing strategy achieved near-perfect 34/33/33% distribution across $N=1000$ Monte Carlo runs, resolving the accuracy paradox inherent in GNSS-dominated operational data.

Future work will expand validation through multi-operator measurement campaigns across diverse network architectures, investigate continuous parameter calibration using online field data to reduce the sim-to-real gap, and explore transfer learning techniques enabling models trained on one network's simulation to generalize across heterogeneous deployments. Ultimately, this framework serves as a critical bridge between theoretical ML research and the stringent reliability requirements of next-generation telecommunications infrastructure.

References

- [1] G. P. Sharma et al., "Toward Deterministic Communications in 6G Networks: State of the Art, Open Challenges and the Way Forward," IEEE Access, vol. 11, pp. 106898–106923, 2023.
- [2] D. Chandramouli, P. Andrés-Maldonado, and T. Kolding, "Evolution of Timing Services From 5G-A Toward 6G," IEEE Access, vol. 11, pp. 35150–35157, 2023.
- [3] T. Iliev and I. Penkov, "AI-Driven Trust Score-Based Synchronization Control for Robust 5G and Beyond Networks," in Proc. ICAI 2025, pp. 504–509.
- [4] M. Lévesque and D. Tipper, "A Survey of Clock Synchronization Over Packet-Switched Networks," IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2926–2947, 2016.
- [5] C. Zhang et al., "Three-Way Selection Random Forest Optimization Model for Anomaly Traffic Detection," Electronics, vol. 12, no. 8, p. 1788, 2023.
- [6] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," IEEE Std 1588-2019, Jun. 2020.
- [7] G. Giorgi, "An Event-Based Kalman Filter for Clock Synchronization," IEEE Trans. Instrum. Meas., vol. 64, no. 2, pp. 449–457, 2015.
- [8] A. Nasrallah et al., "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 88–145, 2019.
- [9] F. Girela-López et al., "IEEE 1588 High Accuracy Default Profile: Applications and Challenges," IEEE Access, vol. 8, pp. 45211–45220, 2020.
- [10] Z. Wang et al., "Time Synchronization for 5G and TSN Integrated Networking," IEEE J. Sel. Areas Commun., vol. 43, no. 9, pp. 2969–2980, 2025.
- [11] Y.-D. Seo et al., "Improved Time-Synchronization Algorithm Based on Disturbance Compensation," Sensors, vol. 19, no. 16, p. 3499, 2019.
- [12] P. Assimakopoulos et al., "A Converged Evolved Ethernet Fronthaul for the 5G Era," IEEE JSAC, vol. 36, no. 11, pp. 2528–2537, 2018.

Homomorphic Encryption for Secure Federated Learning: A Narrative Survey

Dinko Dinkov

Nikola Vaptsarov Naval Academy, Varna, Bulgaria

d.dinkov@naval-acad.bg

Abstract: Federated learning enables collaborative model training without data centralization but remains vulnerable to information leakage, model manipulation, and aggregation attacks. This narrative review analyses security challenges through the confidentiality, integrity, and availability (CIA) triad, covering architectures, threat models, and privacy-preserving techniques. Differential privacy and secure multi-party computation are briefly noted, while homomorphic encryption is emphasized as the primary cryptographic solution. Security guarantees and performance trade-offs are assessed, identifying homomorphic encryption as a practical approach for strong confidentiality with minimal accuracy loss. The review provides a design-oriented synthesis of current research and forms the conceptual basis for a complementary PRISMA-based systematic review presented in the second part of this study.

Keywords: homomorphic encryption, network security, federated learning, narrative review.

Received 10 September 2025

Accepted 25 November 2025

Published 19 December 2025

1. Introduction

Interest in homomorphic encryption (HE) grew significantly between 2020 and 2025, both in scientific literature and in industrial applications, especially in the context of federated machine learning. Market analyses by Dimension Market Research [1] show steady growth in the economic value of technologies and solutions based on HE (Figure 1). The global market for HE – including software, services, and solutions that use this technology – is estimated at approximately \$217 million in 2025, with forecasts reaching approximately \$445 million by 2034, at an average annual growth rate of approximately 8–9%. The main drivers of this growth are sectors with high security and regulatory compliance requirements, such as financial services, healthcare, and public administration, where HE allows for simultaneous compliance with regulations and extraction of value from data.

The rapid expansion of data generation and artificial intelligence applications [2] has intensified privacy requirements [3, 4]. Regulations such as the GDPR, HIPAA and national cybersecurity laws increasingly restrict centralized processing of sensitive data. Gartner reports that by the end of 2024 approximately 75% of the global population is covered by modern data protection regulations, compared to less than 10% in 2010 [5].

Combined with the growing frequency of cyberattacks and data breaches [6], these constraints have resulted in isolated “information islands,” making centralized model training increasingly impractical.

Federated learning (FL) addresses this challenge by enabling collaborative training over distributed data without direct data sharing [7, 8], with the global market estimated at \$120–150 million in 2023 and projected annual growth of around 10% [9].

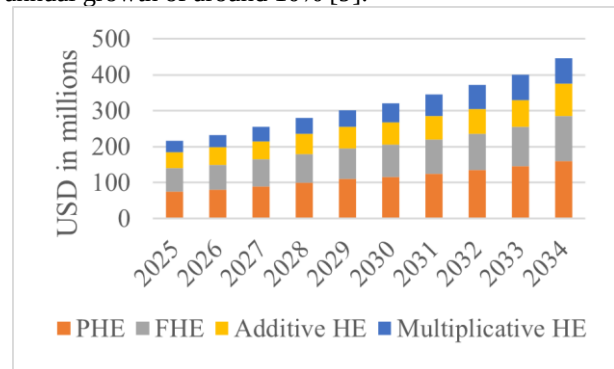


Fig 1. Homomorphic encryption market evaluation.

However, federated learning does not provide inherent security guarantees. Prior work shows that model updates may leak sensitive information [10, 11], while the central aggregator and communication channels remain vulnerable to manipulation and model poisoning attacks [12]. These limitations motivate the integration of cryptographic protection mechanisms, with HE emerging as a promising approach for secure aggregation over encrypted model updates.

2. Federated learning: architecture and learning process

FL is a machine learning paradigm [13] in which multiple distributed clients collaboratively train a shared global model through local computation and periodic exchange of model updates [14]. The aggregation is



performed by a central server, which combines client updates without direct access to raw training data.

Instead of sharing primary data, clients transmit model parameters or gradients to the server, which aggregates them and redistributes the updated global model [15, 16, 17, 18]. This design reduces data exposure by limiting communication to model updates rather than raw data.

The concept of FL was first formalized by Google researchers [8], who introduced the Federated Averaging (FedAvg) algorithm. FedAvg combines local stochastic gradient descent (SGD) on each client [19] with centralized parameter averaging, forming the basis of most contemporary federated learning frameworks.

2.1. Roles

In the classical FL architecture [8], two primary roles are defined: clients and a central server (aggregator). Clients, such as mobile devices, IoT sensors, or institutions, maintain local datasets and perform training on locally stored data using the current global model received from the server [20]. After local optimization, clients transmit their updated model parameters back to the aggregator [20].

The central server coordinates the training process by selecting participating clients, distributing the global model, and aggregating the received updates into a single global model [21]. This aggregation step forms the core mechanism enabling collaborative learning without direct data sharing.

2.2. Learning cycle

The FedAvg algorithm operates in synchronous communication rounds [8]. At each round, the central server selects a subset of available clients and distributes the current global model parameters to them. The selected clients perform local training using SGD over multiple local epochs on their private datasets.

After local computation, clients transmit their model updates to the server, which constructs a new global model through weighted averaging, where each client's contribution is proportional to the size of its local dataset. This iterative process results in a global model trained on the collective knowledge of all participants without requiring raw data to leave local devices.

2.3. Architecture

Depending on the scale, participant characteristics, and available infrastructure, FL can be implemented using different architectural models. The most common are cross-device, cross-silo, and hierarchical architectures, each characterized by distinct assumptions, advantages, and limitations.

Cross-device FL represents the earliest and most widely adopted deployment scenario, initially introduced by Google [8]. It involves a large population of end devices, such as smartphones, IoT sensors, and wearables [22], typically ranging from hundreds to thousands of clients [21]. These devices operate under limited computational and energy resources and often experience unstable network connectivity [23], resulting in dynamic

client participation and partial involvement in each training round.

Cross-silo FL involves a limited number of well-resourced organizations, such as hospitals, financial institutions, or educational entities [24]. Compared to cross-device settings, cross-silo environments benefit from reliable communication infrastructure and substantial computational resources [25], as well as larger and more structured datasets, enabling higher training efficiency and accuracy [26]. As a result, cross-silo FL is expected to achieve performance comparable to centralized or non-encrypted FL while prioritizing strong confidentiality guarantees [27].

Hierarchical FL extends the standard paradigm to improve scalability and efficiency in large-scale and heterogeneous environments, particularly in IoT ecosystems [28, 29]. Training is organized across multiple levels—typically involving end devices, intermediate edge servers, and a central aggregator—where edge servers perform local aggregation before forwarding updates to the central server [30]. This multi-tier architecture reduces communication overhead, lowers latency, and improves resource utilization, while enhancing privacy by keeping data within local domains [29, 31, 32].

3. Security threats in federated learning networks

The CIA triad, confidentiality, integrity, and availability, provides a fundamental framework for analysing security vulnerabilities in FL. Confidentiality risks arise when gradients or model parameters are exchanged in plaintext, enabling inference of sensitive local data. Integrity can be compromised by malicious participants submitting poisoned updates to manipulate training or embed unintended model behavior. Availability, interpreted as the correct aggregation of global model formation, may be threatened by a malicious aggregator or by manipulation of the aggregation process. Together, these dimensions define the primary security threat categories in FL.

3.1. Confidentiality

The primary privacy threat in FL arises from transmitting client updates in plaintext. Although raw data remain local, prior studies demonstrate that sensitive information—including detailed attributes or full reconstructions of training samples—can be inferred from shared gradients [10, 33]. This gradient-based privacy leakage represents a fundamental limitation of standard FL protocols and motivates the integration of additional cryptographic protection mechanisms.

Attacks exploiting gradient leakage in FL include DLG, which reconstructs original training samples by optimizing against observed gradients [10]; membership inference attacks, which determine whether specific records were included in a client's training data [33, 34]; and property inference attacks, which extract statistical or semantic attributes unrelated to the target task [11]. Additional threats include generative adversarial network (GAN)-based reconstruction attacks, in which an active participant generates synthetic samples resembling

private data [35, 36], as well as model inversion attacks, which recover sensitive features from trained models, including advanced generative variants leveraging GANs [37].

3.2. Integrity

While confidentiality concerns the disclosure of sensitive data, integrity threats target the correctness of the FL process itself. Rather than extracting information, attackers aim to manipulate the global model by injecting malicious or corrupted updates. Participants that intentionally or due to compromise submit such updates are commonly referred to as Byzantine clients [38], and their presence can significantly degrade model accuracy, stability, and reliability.

Typical integrity attacks include model poisoning, where gradients or parameters are maliciously modified to disrupt convergence [18]; backdoor attacks, in which a model behaves correctly on benign inputs but exhibits adversarial behavior when specific trigger patterns are present [14]; and Sybil attacks, where a single adversary assumes multiple identities to gain disproportionate influence over the aggregation process [39].

Compromised integrity may result in unpredictable or malicious model behavior, posing severe risks in safety-critical domains such as medical diagnosis, financial decision-making, and fraud detection.

3.3. Availability

Availability threats in FL arise when the aggregation process is manipulated by a compromised or malicious central server. Unlike the *honest-but-curious* assumption, such an aggregator actively deviates from the protocol by modifying, omitting, or injecting updates, potentially resulting in an incorrect or unstable global model [12].

Typical malicious behaviors include partial aggregation through selective omission or replacement of client updates, injection of fabricated (including encrypted) updates, manipulation of aggregation weights to bias training, replay of outdated updates, and inconsistent distribution of global models across clients [12, 15].

These attacks undermine training robustness and may lead to model-level service failure, where the system is unable to produce a reliable global model.

4. Privacy-preserving approaches in federated learning

The identified vulnerabilities in FL indicate that data decentralization alone is insufficient to ensure confidentiality. Accordingly, the literature groups privacy-preserving mechanisms into three primary categories: differential privacy, secure multi-party computation, and homomorphic encryption. The following sections briefly review these approaches, focusing on their security guarantees, computational and communication overhead, and impact on model accuracy.

4.1. Differential privacy

Differential privacy (DP) is a statistical protection mechanism that introduces random noise into model gradients or parameters, ensuring that the presence of

individual training samples cannot be inferred with high probability [40]. DP provides formal mathematical privacy guarantees by bounding information leakage from model outputs [41]. However, achieving strong privacy requires substantial noise injection, which can significantly degrade model accuracy, particularly for small or heterogeneous datasets [42]. While DP is computationally and communication efficient due to its simplicity [42], the inherent trade-off between privacy and model accuracy remains a key limitation.

4.2. Secure multi-party computation

Secure multi-party computation (SMPC) is a cryptographic paradigm that enables multiple participants to jointly compute a function without revealing their private inputs [43]. In FL, this is commonly realized through a distributed aggregation architecture in which several cooperating servers ensure that no single entity gains access to sensitive data [44]. SMPC offers strong confidentiality guarantees, even against active adversaries; however, its practicality is limited by high communication and computational overhead due to multi-round interactions and increasing execution time with the number of participants [45].

4.3. Homomorphic encryption

HE enables clients to encrypt local model updates before transmission, allowing the central server to perform aggregation directly over encrypted data without decryption [46]. The result is decrypted only after computation, providing strong confidentiality guarantees comparable to SMPC but with a simpler, non-interactive architecture. However, HE incurs substantial computational and communication overhead due to the complexity of cryptographic operations and the large size of encrypted gradients, leading to increased latency and network traffic [46]. Unlike differential privacy, HE preserves model accuracy by avoiding noise injection, as aggregation over encrypted data yields results equivalent to those obtained from plaintext updates [42].

4.4. Comparative analysis of privacy mechanisms

A comparative analysis of privacy-preserving mechanisms in FL indicates that HE provides the strongest confidentiality guarantees without compromising model accuracy. While DP offers formal mathematical guarantees, it inevitably degrades model performance due to noise injection, particularly for small or heterogeneous datasets. SMPC achieves strong protection even against active adversaries but suffers from substantial communication overhead and architectural complexity, limiting its scalability in large deployments. In contrast, HE enables aggregation over encrypted parameters without exposing sensitive information to the server and integrates seamlessly into existing FL architectures. Although computationally expensive, HE preserves model accuracy and exhibits better scalability in heterogeneous environments, motivating its selection as the primary cryptographic mechanism considered in this study.

5. Homomorphic encryption

HE enables computations to be performed directly on encrypted data without revealing the underlying plaintext. This property, known as homomorphism, ensures that specific operations on ciphertexts correspond to equivalent operations on the original data. For ciphertexts $Enc(a)$ and $Enc(b)$, operations $\oplus$ and $\otimes$ are defined such that:

$$Enc(a) \oplus Enc(b) = Enc(a + b) \quad (1)$$

$$Enc(a) \otimes Enc(b) = Enc(a \cdot b) \quad (2)$$

In FL, this allows a central server to aggregate encrypted client updates without accessing sensitive information, while the aggregated result remains encrypted and can be decrypted only by authorized key holders.

Although the concept of homomorphic encryption was introduced in 1978 [47], practical realisation became feasible with the first fully homomorphic scheme proposed by Gentry in 2009 [48]. Since then, HE schemes have evolved significantly, achieving improved efficiency and broader applicability, particularly in FL scenarios where secure processing of sensitive data is required.

5.1. Types of homomorphic encryption

HE schemes can be classified based on the set of supported operations. Partially homomorphic encryption (PHE) supports a single operation with unlimited frequency [49]. Representative examples include Paillier, which enables homomorphic addition [50], and RSA or ElGamal, which support homomorphic multiplication [51, 52]. In FL, additive PHE is often sufficient, as the server primarily performs gradient aggregation, after which clients decrypt the aggregated result and compute averages according to the FedAvg algorithm [8].

Leveled HE (LHE) support an arbitrary number of additions and a predefined number of multiplications. These schemes require parameter selection that bounds the computational depth of arithmetic circuits. Notable examples include BFV [53] and BGV [54], which are based on the Ring Learning With Errors problem (RLWE) [55] and offer greater computational expressiveness than PHE while remaining more efficient than fully homomorphic schemes.

Fully homomorphic encryption (FHE) supports unrestricted sequences of addition and multiplication on encrypted data, enabling the evaluation of arbitrary functions without decryption. The first FHE construction was introduced by Gentry in 2009 [48]. Modern schemes are optimized for different workloads, such as CKKS for approximate arithmetic commonly used in machine learning [56] and TFHE for efficient Boolean operations [57]. Despite their expressiveness, FHE schemes incur substantial computational overhead, limiting their practicality in large-scale or resource-constrained environments.

5.2. Ciphertext noise and bootstrapping

Modern FHE schemes are based on the RLWE problem [55], where security relies on the introduction of controlled noise. Each ciphertext includes a random noise

component that ensures semantic security, producing different ciphertexts for repeated encryptions of the same message. During homomorphic computation, this noise accumulates—linearly under addition and exponentially under multiplication [48]—thereby imposing a scheme-specific noise threshold that limits computational depth. Exceeding this threshold results in incorrect decryption.

Bootstrapping, introduced by Gentry [48], refreshes ciphertexts by homomorphically evaluating the decryption function, effectively reducing accumulated noise and enabling further computation. However, bootstrapping is computationally expensive and often constitutes the primary performance bottleneck in FHE systems. Consequently, many practical implementations restrict circuit depth and operate in LHE modes to balance correctness and efficiency [43].

5.3. Homomorphic encryption optimization techniques

The primary challenge in applying HE to FL lies in its high computational and communication overhead. To address these limitations, the literature identifies three main optimization directions—algorithmic, hardware, and hybrid, whose adoption is essential for making HE practical in real-world deployments [58].

Algorithmic optimizations focus on reducing computation and communication costs across FL phases. Techniques such as quantization compress high-precision gradients to reduce data transmission [41], while methods like BatchCrypt combine quantization with efficient encoding [59]. Packing and batching techniques, including Chinese Remainder Theorem (CRT) and polynomial packing [60], enable multiple gradients to be processed within a single ciphertext, and SIMD-style optimizations in schemes such as CKKS allow parallel computation.

Hardware optimizations accelerate computationally intensive HE operations, such as modular arithmetic. FPGA- and GPU-based solutions exploit parallelism to improve performance, while CPU-level optimizations using libraries such as Intel HEXL leverage SIMD instructions to enhance efficiency even without specialized hardware [61].

Hybrid approaches combine HE with complementary mechanisms such as DP or secret sharing (SS) to balance security, efficiency, and accuracy. HE-DP schemes reduce cryptographic parameter sizes by leveraging noise for additional protection [62], while HE-SS combinations improve resistance to collusion in scenarios where pure FHE is impractical [63].

5.4. Key management

Cryptographic key management is a critical component in integrating HE into FL, as it directly affects both confidentiality and system interoperability [42]. Since homomorphic operations require ciphertexts to be encrypted under the same key, careful selection of the key management model is essential.

The shared-key approach employs a common public key for encryption and a shared private key for decryption across all clients [64]. This model ensures full ciphertext interoperability and enables straightforward

homomorphic aggregation without additional protocols [18]. However, it introduces a single point of failure: compromise of the shared secret key – through leakage or collusion – results in complete disclosure of all client updates [65]. Moreover, client possession of the private key increases the risk of unauthorized decryption by malicious participants [22], limiting this approach to highly trusted environments.

Threshold cryptography distributes the secret key into multiple shares using schemes such as Shamir Secret Sharing [31, 66], requiring a predefined threshold of participants to cooperatively decrypt the aggregated result [22]. This eliminates single points of compromise and improves resistance to collusion, as neither individual clients nor the server possesses the full key [15, 25]. The main limitation lies in increased computational and communication overhead, since threshold decryption requires multi-party coordination at each iteration, reducing scalability in large or IoT-heavy federated settings [22].

The multi-key (client-specific key) approach assigns each client an independent key pair, thereby avoiding shared secrets and significantly strengthening confidentiality [67]. To enable aggregation, ciphertexts encrypted under different keys are converted into a common key domain via key switching without decryption, using client-generated switching keys [68]. The aggregated ciphertext typically requires coordinated decryption involving multiple private keys, enhancing resistance to collusion [69]. Some implementations further employ proxy re-encryption to facilitate key transformation by a trusted intermediary without exposing plaintexts [70]. While offering strong security, this approach incurs additional cryptographic complexity and communication overhead.

6. Discussion

This narrative survey shows that while FL mitigates risks associated with centralized data collection, it does not inherently guarantee confidentiality, integrity, or availability. Achieving secure federated learning requires additional protection mechanisms that introduce unavoidable trade-offs between privacy strength, computational overhead, and scalability. Differential privacy, secure multi-party computation, and homomorphic encryption each address different aspects of this trade-off, indicating that security in federated learning must be treated as a system-level design challenge rather than a purely cryptographic problem.

Furthermore, the suitability of privacy-preserving mechanisms is strongly influenced by the underlying federated learning architecture. Resource-constrained cross-device environments limit the applicability of computationally intensive schemes, whereas cross-silo and hierarchical settings are better aligned with homomorphic encryption and advanced key management strategies. At the same time, most existing approaches primarily protect confidentiality, while integrity and availability threats remain insufficiently addressed. The diversity of assumptions, architectures, and evaluation criteria across literature complicates direct comparison, motivating the need for a systematic, PRISMA-based

analysis of homomorphic encryption approaches, presented in the second part of this study.

7. Conclusion

This survey examined the security challenges of federated learning from a system and threat-oriented perspective, with emphasis on confidentiality, integrity, and availability. By analyzing federated learning architectures, threat models, and privacy-preserving mechanisms, the study highlighted the limitations of data decentralization alone and the necessity of additional cryptographic protection. A comparative discussion of differential privacy, secure multi-party computation, and homomorphic encryption showed that homomorphic encryption offers a compelling balance between strong confidentiality and preservation of model accuracy, despite its computational cost. These findings establish a conceptual foundation for the systematic review presented in Part II, which applies the PRISMA methodology to comprehensively analyze homomorphic encryption-based federated learning solutions and identify open research challenges.

References

- [1] Dimension Market Research (2025). Homomorphic Encryption Market Size, Forecasts and Trends Report (June 2025), Dimension Market Research, Available at: <https://dimensionmarketresearch.com/report/homomorphic-encryption-market/#overview/> (accessed 05 Dec. 2025).
- [2] Jenkin, D. (2025). How much data is created every day: key insights & trends, DesignRush, Available at: <https://www.designrush.com/agency/big-data-analytics-companies/trends/how-much-data-is-created-every-day>.
- [3] Gheisari, M. et al. (2023). Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey, *CAAI Transactions on Intelligence Technology*, vol. 8, no. 3, pp. 581-606, <https://doi.org/10.1049/cit2.12180>.
- [4] Jabeen, S., Li, X., Amin, M. S., Bourahla, O., Li, S. & Jabbar, A. (2023). A review on methods and applications in multimodal deep learning, *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 19, no. 2s, pp. 1-41, <https://doi.org/10.1145/3545572>.
- [5] Gartner (2022). Gartner identifies top five trends in privacy through 2024, *Gartner*, Available at: <https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024> (accessed 05 Dec. 2025).
- [6] Booth, R. (2025). Cyber-attacks rise by 50% in past year, UK security agency says, *The Guardian*, Available at: <https://www.theguardian.com/technology/2025/oct/14/cyber-attacks-rise-in-past-year-uk-security-agency-says> (accessed 05 Dec. 2025).
- [7] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T. & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency, *arXiv preprint*, arXiv:1610.05492, <https://arxiv.org/abs/1610.05492>.
- [8] McMahan, B., Moore, E., Ramage, D., Hampson, S. & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data, *Artificial Intelligence and Statistics (AISTATS)*, PMLR, pp. 1273-1282.
- [9] Allied Market Research (2024). Federated Learning Solutions Market Size, Share, Competitive Landscape and Trend Analysis Report, by Component (Solution, Services), by Application, by Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2024-2032, *Allied Market Research*,

Available at: <https://www.alliedmarketresearch.com/federated-learning-solutions-market-A14591> (accessed 05 Dec. 2025).

- [10] Zhu, L., Liu, Z. & Han, S. (2019). Deep leakage from gradients, *Proceedings of the 33rd International Conference on Neural Information Processing Systems (NeurIPS)*, Curran Associates Inc., pp. 14774-14784.
- [11] Melis, L., Song, C., De Cristofaro, E. & Shmatikov, V. (2019). Exploiting unintended feature leakage in collaborative learning, *2019 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 691-706, doi: 10.1109/SP.2019.00029.
- [12] Gao, H., He, N. & Gao, T. (2023). SVeriFL: Successive verifiable federated learning with privacy-preserving, *Information Sciences*, vol. 622, pp. 98-114, <https://doi.org/10.1016/j.ins.2022.11.124>.
- [13] Fontenla-Romero, O., Guijarro-Berdiñas, B., Hernández-Pereira, E. & Pérez-Sánchez, B. (2023). FedHEONN: Federated and homomorphically encrypted learning method for one-layer neural networks, *Future Generation Computer Systems*, vol. 149, pp. 200-211, <https://doi.org/10.1016/j.future.2023.07.018>.
- [14] Chen, X., Tian, Y., Wang, S., Yang, K., Zhao, W. & Xiong, J. (2025). DBFL: Dynamic Byzantine-Robust Privacy Preserving Federated Learning in Heterogeneous Data Scenario, *Information Sciences*, vol. 700, Art. No. 121849, <https://doi.org/10.1016/j.ins.2024.121849>.
- [15] Lai, P., Zhang, M., Tang, Y., Yue, Y. & Di, F. (2025). VPAFL: Verifiable Privacy-Preserving Aggregation for Federated Learning Based on Single Server, *Computers, Materials & Continua*, vol. 84, no. 2, pp. 2935-2957, <https://doi.org/10.32604/cmc.2025.065887>.
- [16] Mohandas, R., Veena, S., Kirubasri, G., Thusnavis Bella Mary, I. & Udayakumar, R. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data, *Indian Journal of Information Sources and Services*, vol. 14, no. 2, pp. 17-23, <https://doi.org/10.51983/ijiss-2024.14.2.03>.
- [17] Stripelis, D., Gupta, U., Saleem, H., Dhinagar, N., Ghai, T., Anastasiou, C., Sánchez, R., Ver Steeg, G., Ravi, S., Naveed, M., Thompson, P. M. & Ambite, J. L. (2024). A federated learning architecture for secure and private neuroimaging analysis, *Patterns*, vol. 5, no. 8, Art. No. 101031, <https://doi.org/10.1016/j.patter.2024.101031>.
- [18] Xu, R., Gao, S., Li, C., Joshi, J. & Li, J. (2024). Dual defense: Enhancing privacy and mitigating poisoning attacks in federated learning, *Advances in Neural Information Processing Systems*, vol. 37, pp. 70476-70498, doi: 10.52202/079017-2253.
- [19] Robbins, H. & Monro, S. (1951). A Stochastic Approximation Method, *The Annals of Mathematical Statistics*, vol. 22, no. 3, pp. 400-407, <https://doi.org/10.1214/aoms/1177729586>.
- [20] Li, L., Sun, X., Shi, N., Ci, X. & Liang, C. (2024). A Stealthy Communication Model for Protecting Aggregated Results Integrity in Federated Learning, *Electronics*, vol. 13, no. 19, p. 3870, <https://doi.org/10.3390/electronics13193870>.
- [21] Asiri, M., Khemakhem, M. A., Alhebshi, R. M., Alsulami, B. S. & Eassa, F. E. (2025). RPFL: A Reliable and Privacy-Preserving Framework for Federated Learning-Based IoT Malware Detection, *Electronics*, vol. 14, no. 6, p. 1089, <https://doi.org/10.3390/electronics14061089>.
- [22] Park, J. & Lim, H. (2022). Privacy-Preserving Federated Learning Using Homomorphic Encryption, *Applied Sciences*, vol. 12, no. 2, p. 734, <https://doi.org/10.3390/app12020734>.
- [23] He, Y., Wei, L., Chen, F., Zhang, H., Yu, J. & Wang, H. (2025). FedAI: Federated recommendation system with anonymized interactions, *Expert Systems with Applications*, vol. 271, Art. No. 126564, <https://doi.org/10.1016/j.eswa.2025.126564>.
- [24] Zhang, C., Zhang, X., Yang, X., Liu, B., Zhang, Y. & Zhou, R. (2025). Poisoning attacks resilient privacy-preserving federated learning scheme based on lightweight homomorphic encryption, *Information Fusion*, vol. 121, Art. No. 103131, <https://doi.org/10.1016/j.inffus.2025.103131>.
- [25] Bouamama, J., Benkaouz, Y. & Ouzzif, M. (2025). V-FLEX: Verifiable cross-silo federated learning using trusted execution environment, *Progress in Artificial Intelligence*, <https://doi.org/10.1007/s13748-025-00386-9>.
- [26] Rieyan, S. A., Alam, M. M., Alzain, M. A. & Rahman, M. M. (2024). An advanced data fabric architecture leveraging homomorphic encryption and federated learning, *Information Fusion*, vol. 102, Art. No. 102004, <https://doi.org/10.1016/j.inffus.2024.102004>.
- [27] Angulo, E., Márquez, J. & Villanueva-Polanco, R. (2023). Training of Classification Models via Federated Learning and Homomorphic Encryption, *Sensors*, vol. 23, no. 4, p. 1966, <https://doi.org/10.3390/s23041966>.
- [28] Gu, C. & Li, B. C. (2024). Hierarchical federated learning architectures for the metaverse, *ZTE Communications*, vol. 22, no. 2, pp. 39-48, <https://doi.org/10.12142/ZTECOM.202402006>.
- [29] Alzaharani, B. & Yang, D. (2025). PrivHFL: A privacy-preserving scheme for hierarchical federated learning, *Computer Networks*, vol. 273, Art. No. 111764, <https://doi.org/10.1016/j.comnet.2025.111764>.
- [30] Wang, H., Feng, J., Bu, M., Ding, Y., Tang, S. & Yang, C. (2025). MVFL: verifiable privacy-preserving federated learning using multi-key homomorphic encryption, *The Journal of Supercomputing*, vol. 81, no. 8, p. 915, <https://doi.org/10.1007/s11227-025-07419-z>.
- [31] Cao, S., Liu, S., Yang, Y., Du, W., Zhan, Z., Wang, D. & Zhang, W. (2025). A hybrid and efficient Federated Learning for privacy preservation in IoT devices, *Ad Hoc Networks*, vol. 170, Art. No. 103761, <https://doi.org/10.1016/j.adhoc.2025.103761>.
- [32] Wang, B. & Yang, F. (2024). Lightweight and privacy-preserving hierarchical federated learning mechanism for artificial intelligence-generated image content, *Journal of Real-Time Image Processing*, vol. 21, no. 4, Art. No. 149, <https://doi.org/10.1007/s11554-024-01524-7>.
- [33] Shokri, R., Stronati, M., Song, C. & Shmatikov, V. (2017). Membership inference attacks against machine learning models, *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 3-18, <https://doi.org/10.1109/SP.2017.41>.
- [34] Nasr, M., Shokri, R. & Houmansadr, A. (2019). Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning, *2019 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 739-753, <https://doi.org/10.1109/SP.2019.00065>.
- [35] Hitaj, B., Ateniese, G. & Perez-Cruz, F. (2017). Deep models under the GAN: Information leakage from collaborative deep learning, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, ACM, pp. 603-618, <https://doi.org/10.1145/3133956.3134012>.
- [36] Wang, Z., Song, M., Zhang, Z., Song, Y., Wang, Q. & Qi, H. (2019). Beyond inferring class representatives: User-Level Privacy Leakage From Federated Learning, *2019 IEEE Conference on Computer Communications (INFOCOM)*, IEEE, pp. 2512-2520, <https://doi.org/10.1109/INFOCOM.2019.8737416>.
- [37] Fredrikson, M., Jha, S. & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*, ACM, pp. 1322-1333, <https://doi.org/10.1145/2810103.2813677>.
- [38] Zhou, A., Jiang, N. & Tang, T. (2024). Asynchronous Robust Aggregation Method with Privacy Protection for IoV Federated Learning, *World Electric Vehicle Journal*, vol. 15, no. 1, p. 18, <https://doi.org/10.3390/wevj15010018>.

- [39] Deng, Y., Guo, B. & Chen, S. (2025). Privacy-Preserving Approach to Edge Federated Learning Based on Blockchain and Fully Homomorphic Encryption, *Electronics*, vol. 14, no. 2, p. 361, <https://doi.org/10.3390/electronics14020361>.
- [40] Manzoor, H. U., Shabbir, A., Chen, A., Flynn, D. & Zoha, A. (2024). A survey of security strategies in federated learning: Defending models, data, and privacy, *Future Internet*, vol. 16, no. 10, p. 374, <https://doi.org/10.3390/fi16100374>.
- [41] Aziz, R., Banerjee, S., Bouzeffrane, S. & Le Vinh, T. (2023). Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm, *Future Internet*, vol. 15, no. 9, p. 310, <https://doi.org/10.3390/fi15090310>.
- [42] Xin, W., Jiaqian, L., Xueshuang, D., Haoji, Z. & Lianshan, S. (2025). A survey of differential privacy techniques for federated learning, *IEEE Access*, vol. 13, pp. 6539-6555, <https://doi.org/10.1109/ACCESS.2024.3523909>.
- [43] Feretakis, G., Papaspyridis, K., Gkoulalas-Divanis, A. & Verykios, V. S. (2024). Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review, *Information*, vol. 15, no. 11, p. 697, <https://doi.org/10.3390/info15110697>.
- [44] Stan, O., Thouvenot, V., Boudguiga, A., Kapusta, K., Zuber, M. & Sirdey, R. (2022). A Secure Federated Learning: Analysis of Different Cryptographic Tools, *Proceedings of the 19th International Conference on Security and Cryptography (SECRYPT)*, SciTePress, pp. 669-674, <https://doi.org/10.5220/0011322700003283>.
- [45] Liu, F., Zheng, Z., Shi, Y., Tong, Y. & Zhang, Y. (2024). A survey on federated learning: a perspective from multi-party computation, *Frontiers of Computer Science*, vol. 18, Art. No. 181336, <https://doi.org/10.1007/s11704-023-3282-7>.
- [46] Shalabi, E., Khedr, W., Rushdy, E. & Salah, A. (2025). A comparative study of privacy-preserving techniques in federated learning: A performance and security analysis, *Information*, vol. 16, no. 3, p. 244, <https://doi.org/10.3390/info16030244>.
- [47] Rivest, R. L., Adleman, L. & Dertouzos, M. L. (1978). On Data Banks and Privacy Homomorphisms, in R. A. DeMillo, D. P. Dobkin, A. K. Jones & R. J. Lipton (Eds.), *Foundations of Secure Computation*, vol. 4, Academic Press, pp. 169-180.
- [48] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*, ACM, pp. 169-178, <https://doi.org/10.1145/1536414.1536440>.
- [49] Munjal, K. & Bhatia, R. (2022). Analysing RSA and PAILLIER homomorphic Property for security in Cloud, *Procedia Computer Science*, vol. 215, pp. 240-246, <https://doi.org/10.1016/j.procs.2022.12.027>.
- [50] Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, *Advances in Cryptology — EUROCRYPT '99*, Lecture Notes in Computer Science, vol. 1592, Springer, pp. 223-238, https://doi.org/10.1007/3-540-48910-X_16.
- [51] Rivest, R. L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, <https://doi.org/10.1145/359340.359342>.
- [52] ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, <https://doi.org/10.1109/TIT.1985.1057074>.
- [53] Fan, J. & Vercauteren, F. (2012). Somewhat practical fully homomorphic encryption, *IACR Cryptology ePrint Archive*, Paper 144, Available at: <https://eprint.iacr.org/2012/144>.
- [54] Brakerski, Z., Gentry, C. & Vaikuntanathan, V. (2012). (Leveled) fully homomorphic encryption without bootstrapping, *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS)*, ACM, pp. 309-325, <https://doi.org/10.1145/2090236.2090262>.
- [55] Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*, ACM, pp. 84-93, <https://doi.org/10.1145/1060590.1060603>.
- [56] Cheon, J. H., Kim, A., Kim, M. & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers, *Advances in Cryptology – ASIACRYPT 2017*, Lecture Notes in Computer Science, vol. 10624, Springer, pp. 409-437, https://doi.org/10.1007/978-3-319-70694-8_15.
- [57] Chillotti, I., Gama, N., Georgieva, M. & Izabachène, M. (2020). TFHE: Fast fully homomorphic encryption over the torus, *Journal of Cryptology*, vol. 33, no. 1, pp. 34-91, <https://doi.org/10.1007/s00145-019-09319-x>.
- [58] Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., Dai, W., Liu, Z. & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey, *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 24569-24580, <https://doi.org/10.1109/JIOT.2024.3382875>.
- [59] Zhang, C., Li, S., Xia, J., Wang, W., Yan, F. & Liu, Y. (2020). BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning, *Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC)*, USENIX Association, pp. 493-506.
- [60] Childs, L. N. (1995). The Chinese Remainder Theorem, *A Concrete Introduction to Higher Algebra*, Undergraduate Texts in Mathematics, Springer, pp. 194-207, https://doi.org/10.1007/978-1-4419-8702-0_12.
- [61] Intel Labs (2025). HEXL: High-Performance Homomorphic Encryption Library, *Intel Labs*, Available at: <https://github.com/IntelLabs/hexl> (accessed 14 Nov. 2025).
- [62] Zhao, J., Huang, C., Wang, W., Xie, R., Dong, R. & Matwin, S. (2023). Local differentially private federated learning with homomorphic encryption, *The Journal of Supercomputing*, vol. 79, pp. 19365-19395, <https://doi.org/10.1007/s11227-023-05378-x>.
- [63] Ming, Y., Wang, S., Wang, C., Liu, H., Deng, Y., Zhao, Y. & Feng, J. (2024). VCSA: Verifiable and collusion-resistant secure aggregation for federated learning using symmetric homomorphic encryption, *Journal of Systems Architecture*, vol. 156, Art. No. 103279, <https://doi.org/10.1016/j.sysarc.2024.103279>.
- [64] Liang, X., Xu, Y., Lin, Y., Zhang, C. (2025). Federated split learning via dynamic aggregation and homomorphic encryption on non-IID data, *The Journal of Supercomputing*, vol. 81, Art. No. 63, <https://doi.org/10.1007/s11227-024-06612-w>.
- [65] Bai, F., Zhao, Y., Shen, T., Zeng, K., Zhang, X. & Zhang, C. (2025). FedOPCS: An optimized poisoning countermeasure for non-IID federated learning with privacy-preserving stability, *Symmetry*, vol. 17, no. 5, p. 782, <https://doi.org/10.3390/sym17050782>.
- [66] Shamir, A. (1979). How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, <https://doi.org/10.1145/359168.359176>.
- [67] Liu, Q.-X., Zhang, J.-G. & Tan, B. (2024). Financial fraud recognition model based on privacy preserving and federated learning, *Journal of Network Intelligence*, vol. 9, no. 4, pp. 2360-2374.
- [68] Liu, Z., Chen, S., Ye, J., Fan, J., Li, H. & Li, X. (2022). DHSA: Efficient doubly homomorphic secure aggregation for cross-silo federated learning, *The Journal of Supercomputing*, vol. 79, pp. 2819-2849, <https://doi.org/10.1007/s11227-022-04745-4>.
- [69] Ma, J., Naas, S.-A., Sigg, S. & Lyu, X. (2022). Privacy-preserving federated learning based on multi-key homomorphic

encryption, *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 5880-5901, <https://doi.org/10.1002/int.22818>.
[70] Wei, Z., Wang, J., Zhao, Z. & Zhao, Z. (2025). Byzantine-robust federated learning considering distributed

Non-IID data in privacy-sensitive scenarios, *Information Fusion*, vol. 124, Art. No. 103345, <https://doi.org/10.1016/j.inffus.2025.103345>.

Intentional Interaction for Screenless Rectangular AI Wearables via Dual-Side Touch

Yuri Dimitrov

Technical University of Varna, Varna, Bulgaria

yndimitrov@gmail.com

Abstract The development of human-computer interaction for wearables is driven by two major factors. Firstly, there has been a proliferation of screenless AI assistants. Secondly, there have been heightened privacy concerns regarding "always-listening" models. A theoretical framework is proposed for manual activation to ensure voice-based communication is initiated only through deliberate intent. A rectangular device with opposite-side touch interfaces is utilised to facilitate eyes-free command execution. The two-finger "grasp" algorithm has been developed to ensure reliable activation and navigation, including volume control, playback rollback, and deactivation. User privacy and energy efficiency are prioritised, whilst the necessity for visual confirmation is eliminated and unauthorised data collection is mitigated.

Keywords: Wearable, Screenless Interface, AI Assistant, Two-finger Touch, Privacy.

Received 10 November 2025

Accepted 5 December 2025

Published 12 January 2025

1. Introduction

In recent years, the proliferation of wearable devices has precipitated their entry into the mainstream market, thereby constituting a substantial segment of the global technology economy [1]. The global wearable technology market was valued at approximately USD 55.5 billion in 2022 [1]. Projections indicate that this figure will reach USD 142.4 billion by 2030. These systems currently possess greater computational power, memory and communication capabilities than average personal computers did two decades ago [2]. Notwithstanding this continuous technical refinement, user-device interaction techniques remain largely analogous to those observed in classic electronic watches or smartphones. However, as devices become smaller to remain socially acceptable and unobtrusive, they encounter the 'fat finger' problem, whereby the user's own finger inevitably obscures the visual interface or small target icons during interaction [3].

The physical form of wrist-worn devices imposes limitations on the number of mechanical input devices with which they can be equipped, and their diminutive screen size imposes further restrictions on the amount of textual and graphical information they can display [4]. Alphanumeric user interfaces utilising typed commands are deemed unsuitable for this domain, owing to the lack of available space on the device to implement a standard keyboard. The advent of voice-centric AI assistants has precipitated an escalating adoption of screenless designs within the industry [2, 5]. Nevertheless, this transition has given rise to substantial concerns regarding user privacy,

as 'always-listening' microphones are generally necessary for voice activation. It has been posited that intuitive, trustworthy AI-human interfaces must strike a balance between efficiency and transparency in order to mitigate user anxiety regarding unauthorised data collection [6].

The defining characteristic of traditional wearables is their rigidity, which often results in an inability to establish reliable, conforming contact with the human body's curved surfaces [1]. Contemporary research in this field is focused on the development of thinner, smaller and more unobtrusive devices [1]. The reduced screen size of wrist-worn devices renders graphical user interfaces (GUIs) dependent on cursor manipulation unsuitable, as these require significant visual attention, which can pose a problem in mobile settings where the user must be aware of their surroundings [4]. It is therefore proposed that a rectangular form factor with dual-sided touch sensors be utilised to enable eyes-free intentional command execution and improved privacy. The activation of the system necessitates a deliberate manual action, thereby preserving battery life while the system remains in power-saving mode [7]. Moreover, high-power modules, such as hardware accelerators for neural network inference, can remain dormant until user intent is confirmed physically [8].

2. Related Work

Researchers have extensively explored surfaces beyond the display for human-computer interaction (HCI) to mitigate line-of-sight obstruction on small displays [5, 9]. The interaction between the perpendicular edges of a device has been evaluated to ensure that the user's fingers and the screen remain clearly visible during targeting operations [9]. It is evident that major vendors have implemented mechanical solutions, including rotating



© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

bezels and digital crowns, in order to address the issue of 'fat fingers' [2]. However, these solutions typically necessitate a conventional button press for initial activation, thus failing to address the requirement for an instant, gesture-based wake-up [7].

Research into alternative sensing areas has expanded the input expressivity of smartwatches. These include pressure-sensitive multi-touch interaction on a wristband (BandSense), which provides a more expansive interaction area with reduced occlusion [10]. Interacting with the back of the device (nanoTouch) has been proposed as a method of eliminating interference between the fingers and the screen. This method of visual feedback is intended to inform the user of their finger position via an on-screen pointer or pseudo-transparency [5]. A number of studies have explored the potential of utilising side-pressure sensors (PressTact) to facilitate bi-directional navigation, including functions such as zooming and scrolling, by employing varying levels of force [11].

As indicated in the preceding research carried out at the Technical University of Varna, a substantial foundation has been laid concerning the effectiveness of bezel-based interaction. Research has demonstrated that fundamental interface operations can be identified through the utilisation of a two-finger touch on the device bezel [12]. Initial studies employed a 3D-printed smartwatch model, measuring 44 mm in diameter, which was equipped with capacitive sensors connected to an Arduino Mega 2560 and an MPR121 extension board [12]. It was determined that during a manual "grasp," sufficient non-touched space (specifically two or more sensors) exists between the thumb and index finger to unambiguously detect a deliberate action in 100% of user attempts [7]. This finding is critical for distinguishing intentional activation from accidental contact with clothing or skin [7].

Subsequent development of this paradigm resulted in the creation of a "Novel" interface, which was compared to a "Standard" model featuring side push buttons [13]. The Novel interface incorporated a 46 mm 3D-printed chassis, with the bezel itself serving as the primary input surface [12]. Research findings demonstrated that scrolling actions for menu navigation could be recognised with a high degree of stability, requiring a minimum of two sensor transitions per gesture attempt [12]. In comparative studies, it was found that the Novel touch interface outperformed the Standard button-based model in terms of operation speed. Specifically, execution times for complex command sequences were found to be 9.56% faster when using the touch-based approach [13].

The feasibility of eyes-free command execution, such as "Up", "Down", "Enter" and "Back", was confirmed through the development of specialised Arduino software that processed simultaneous inputs from multiple sensors to distinguish between a static "support" finger and an "active" moving finger [12, 13]. It was observed that while the Novel interface initially exhibited a higher error rate due to user familiarity with traditional buttons, the performance benefit increased as the set of commands became longer and more complex [13]. Furthermore, research into user pose recognition has indicated that the symmetrical results of touch zones allow for the determination of the user's physical state [standing, sitting,

and lying] based on the probability of specific sensors being activated [14]. A range of techniques, including tilting operations, have been examined with a view to expanding input vocabularies. The results of this research demonstrate that, in general, greater accuracy is achieved through the inclination of the arm (x-axis) than through the rotation of the wrist (y-axis) [15]. However, these sensors frequently necessitate the user to strike specific angular targets, which can be obscured by the finger depending on the quadrant of the watch face [16]. The present study extends these findings by adapting the dual-touch model to a screenless rectangular chassis designed specifically for intentional AI assistant control and eyes-free parameter adjustment.

3. Materials and Methods

3.1. Hardware Architecture

The experimental prototype was driven by an Arduino Mega 2560 microcontroller [12]. The capacitive sensing process was facilitated by an MPR121 extension board, which featured 12 sensing ports, as demonstrated on Fig 1. The device body was manufactured using 3D printing with white PETG material, chosen to mimic the aesthetics of commercial wearables [7]. The sensors were constructed from steel elements with rounded ends, thus ensuring a smooth tactile surface across the opposite sides of the rectangular frame [12]. The maintenance of data integrity was ensured through the implementation of e-shielded cabling, a measure employed to mitigate electromagnetic interference emanating from the user's body [13].



Fig. 1. Internal view of the rectangular prototype showing the MPR121 board and internal wiring.

3.2. Software Development

Specialised software was developed for the Arduino platform to facilitate the experiments [12]. The software was developed utilising the Arduino programming language (C-based) to detect the initiation (contact) and cessation (release) of each capacitive sensor independently [12]. The algorithm was designed to process simultaneous inputs from multiple sensors to distinguish between a static "support" finger and an "active" moving finger [12]. The real-time data output was facilitated by the Arduino IDE Serial Monitor and subsequently transferred to MS Excel for processing [12].

3.3. Activation and Command Execution Logic

The intentional activation of the device was achieved through the detection of a simultaneous two-finger touch on opposite longitudinal sides. The interface was programmed to transition from idle mode only when a specific temporal threshold of contact was maintained and a minimum non-touched space was recorded [7]. Following activation, the subsequent command set was implemented for the purpose of eyes-free management of the AI assistant [12]:

- **UP/DOWN (Navigation):** A sliding motion along the side sensors while the thumb remained static.
- **VOLUME (Increase/Decrease):** Sliding motion utilised during active audio playback.
- **STOP (Cancel/Mute):** A double-tap on the index finger side.
- **ROLLBACK (Replay last 10 seconds):** A specific reverse sliding gesture.
- **DEACTIVATION:** Immediate return to a low-power "sleep" state upon the release of the thumb contact.

The obtained results are shown in Table 1.

Table 1. Experimental Study Results

User	Activation	UP	STOP	De-Activ.
1 lapel	Successful	Successful	Successful	Successful
2 lapel	Successful	Successful	Successful	Successful
3 lapel	Successful	Successful	Successful	Successful
4 lapel	Successful	Successful	Successful	Successful
5 lapel	Successful	Successful	Successful	Successful
1 belt	Successful	Successful	Successful	Successful
2 belt	Successful	Successful	Successful	Successful
3 belt	Successful	Successful	Successful	Successful
4 belt	Successful	Successful	Successful	Successful
5 belt	Successful	Successful	Successful	Successful

4. Experimental Study

The study was conducted with a group of 5 volunteers in standard office conditions. Participants were required to "grasp" the rectangular device, attached to the lapel, to activate the interface, followed by the execution of pre-defined command sequences without looking at the device as demonstrated on Fig 2.



Fig. 2. A participant's hand performing the dual-side "grasp" on the rectangular prototype on lapel.

The experiment was repeated when the device was attached to the participants' belts. The software recorded the precise sensor identifiers that were triggered, in addition to the duration of each recorded gesture [12]. This facilitated the analysis of performance parameters [13].

5. Results

5.1. Reliability of Activation

The experimental trials that were conducted to investigate this issue conclusively demonstrated that a simultaneous two-finger touch on opposite sides of the rectangular body is unambiguously detectable in 100% of user attempts. The same applies to deactivating the interface by lifting your fingers from the interface areas of the wearable device.

5.2. Feasibility of Command Execution

The feasibility of implementing eyes-free commands for an AI assistant was demonstrated through the recognition of specific tactile gestures. It was established that scrolling actions for navigation or parameter adjustment could be recognised with a high degree of stability, as a minimum of two sensor transitions were recorded in every attempt at a gesture. The execution of discrete commands was confirmed via tap and double-tap gestures. These gestures were processed independently for the active finger. The execution of these commands included increasing volume and stopping communication, increasing volume, and performing a 10-second playback rollback. Finally, the reliability of deactivating the interface was verified, with the system returning to a low-power sleep state immediately upon the release of the thumb contact.

6. Discussion

The transition towards screenless AI wearables necessitates an interface architecture that does not rely on visual confirmation. The findings of this study suggest that the rectangular form factor, which incorporates touch-sensitive zones on opposite longitudinal sides, offers natural tactile landmarks that facilitate effective guidance of user interaction. This architecture addresses the "fat finger" problem by moving the interaction surface away from the visual output, thereby preventing content occlusion [12, 13]. The transfer of interface complexity from the screen to the physical body of the device has been demonstrated to result in a concomitant reduction in cognitive load during interaction.

Moreover, the implementation of a manual, intentional activation method provides a critical solution to contemporary user privacy concerns. The device has been designed in such a way that it can only be activated by a deliberate two-finger grasp, thus ensuring that voice-recognition modules cannot be triggered inadvertently in private or sensitive environments [6]. In principle, this "physical handshake" guarantees that data collection is confined to periods of active user intent, thereby fostering greater user trust in AI systems. Energy efficiency has also been significantly improved; high-power computational modules, such as AI inference accelerators, remain in a

dormant state until the tactile sensors confirm a legitimate grip [7, 8].

The hypothesis that the rectangular chassis is superior to the circular model is evidenced by the clear orientation it provides for spatial memory. Whilst circular bezels permit radial input, the distinct edges of a rectangle function as precise anchor points for the thumb and fingers, thereby enabling high-precision sliding gestures without visual feedback [4, 9]. This tactile guidance enables expert users to execute shortcuts and navigate hierarchical structures with minimal distraction [4]. Although users familiar with traditional button-based interfaces may initially experience a period of adjustment, the theoretical advantage of a continuous touch surface for complex command execution – such as scrolling through vast audio libraries or fine-tuning volume – is substantial [13]. The design has been developed to address the spatial and temporal aspects of the occlusion problem. It has been determined that smaller devices and larger fingers inevitably worsen content occlusion unless the interaction point is offset to the device perimeter [5].

7. Conclusion

A robust method for the intentional manual activation and command execution of screenless wearables has been presented. Through the development of a rectangular prototype, it has been demonstrated that a two-finger grip is a 100% reliable mechanism for waking a device from its idle state while simultaneously providing a secure, privacy-preserving trigger for AI assistants. The execution of commands such as navigation, volume adjustment, and playback rollback without the use of eyes was verified as both technically feasible and efficient.

The broader implications of wearable human-computer interaction (HCI) involve shifting the focus away from visual displays towards tactile and ergonomic ones. The reliability of the proposed dual-side touch interface suggests that it could serve as a primary input modality for future generations of unobtrusive AI assistants. Such systems would facilitate the maintenance of situational awareness by users, whilst concurrently enabling the execution of complex digital tasks through the utilisation of elementary manual gestures. This finding is consistent with the necessity for intuitive and trustworthy AI-human interfaces that enhance human lives through thoughtful design.

The findings indicate that the rectangular form factor is particularly well-suited for eyes-free control, as the physical edges provide consistent landmarks for spatial mapping. Subsequent research endeavours will concentrate on the incorporation of sophisticated machine learning (ML) algorithms with the objective of adapting the interface to the distinct "grasp" patterns exhibited by individual users. This integration has the potential to enhance sensitivity and reduce latency.

Furthermore, the incorporation of pressure-sensitive sensors could lead to a significant augmentation in the input vocabulary, thereby enabling the device to differentiate between varying force levels for multi-dimensional parameter control.

References

- [1] Seng, K. P., Ang, L.-M., Peter, E., and Mmonyi, A. (2023). "Machine Learning and AI Technologies for Smart Wearables," *Electronics*, vol. 12, no. 7, doi: 10.3390/electronics12071509.
- [2] Xiao, R., Laput, G., and Harrison, C. (2014). "Expanding the Input Expressivity of Smartwatches with Mechanical Pan, Twist, Tilt and Click," *CHI '14*, pp. 193–196, doi: 10.1145/2556288.2557017.
- [3] Siek, K. A., Rogers, Y., and Connelly, K. H. (2005). "Fat Finger Worries: How Older and Younger Users Physically Interact with PDAs," *Proc. INTERACT '05*, pp. 267–280.
- [4] Blaskó, G. and Feiner, S. (2004). "An Interaction System for Watch Computers Using Tactile Guidance and Bidirectional Segmented Strokes," *Proc. ISWC '04*, pp. 120–123.
- [5] Baudisch, P. and Chu, G. (2009). "Back-of-Device Interaction Allows Creating Very Small Touch Devices," *CHI 2009*, pp. 1923–1932, doi: 10.1145/1518701.1518995.
- [6] Sundar, A., Russell-Rose, T., Kruschwitz, U., and Machleit, K. (2025). "The AI interface: Designing for the ideal machine-human experience," *Computers in Human Behavior*, vol. 165, doi: 10.1016/j.chb.2024.108539.
- [7] Dimitrov, Y. (2018). "Two-finger touch interface activation method for wearable devices," *ICEST 2018*, pp. 146–149.
- [8] Balaji, A. N. and Peh, L.-S. (2023). "AI-On-Skin: Towards Enabling Fast and Scalable On-body AI Inference for Wearable On-Skin Interfaces," *Proc. ACM Hum.-Comput. Interact.*, vol. 7, no. EICS, doi: 10.1145/3593239.
- [9] Oakley, I. and Lee, D. (2014). "Interaction on the Edge: Offset Sensing for Small Devices," *CHI '14*, pp. 169–178, doi: 10.1145/2556288.2557138.
- [10] Ahn, Y. et al. (2015). "BandSense: Pressure-sensitive Multi-touch Interaction on a Wristband," *CHI EA '15*, pp. 251–254, doi: 10.1145/2702613.2725441.
- [11] Darbar, R., Sen, P. K., and Samanta, D. (2016). "PressTact: Side Pressure-Based Input for Smartwatch Interaction," *CHI '16*, pp. 2431–2438, doi: 10.1145/2851581.2892436.
- [12] Dimitrov, Y. (2018). "Two-finger Touch Interface for Wearable Devices Prototype Model," *Computer Sciences and Technologies*, TU Varna, no. 1, pp. 11–16.
- [13] Dimitrov, Y., Aleksieva, V., and Valchanov, H. (2019). "Wearable Device Interface Comparison," *ELMA 2019*, pp. 575–578, doi: 10.1109/ELMA.2019.8771650.
- [14] Dimitrov, Y. and Aleksieva, V. (2018). "Two-finger touch on wearable device bezel method for user pose recognition," *ACT 2018*, pp. 11–14.
- [15] Shima, K. et al. (2016). "Investigating Accuracy of Tilting Operation on Wrist-worn Devices with Touchscreens," *CHI '16*, doi: 10.1145/2851581.2892377.
- [16] Ashbrook, D., Lyons, K., and Starner, T. (2008). "An Investigation into Round Touchscreen Wristwatch Interaction," *MobileHCI 2008*, pp. 311–314, doi: 10.1145/1409240.1409307.

