International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Lightweight Federated Learning Frameworks for Privacy-Preserving Predictive Analytics in Remote Patient Monitoring: A Systematic Review

D. Sucharitha[1]* and Dr. M. Senthil Kumaran[2]
[1]Research Scholar, [2]Associate Professor
Department of Computer Science and Engineering
Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV) Deemed to be University
Kanchipuram, India

Abstract - Remote patient monitoring (RPM) via Internet of Healthcare Things (IoHT) devices creates a tension between the clinical value of continuous physiological data and the imperative to protect patient privacy. Federated learning (FL) resolves this by enabling collaborative model training without centralising raw data, yet most existing FL frameworks are too resource-intensive for wearable and edge hardware. This paper presents a systematic review of 28 studies (2022–2026), selected from 257 records following PRISMA 2020 guidelines, at the intersection of lightweight FL, privacy preservation, and RPM. We introduce a three-dimensional definition of "lightweight" covering client model size (MS), communication cost (CC), and device energy consumption (EC), and apply it to score ten representative frameworks. A dedicated privacy–accuracy trade-off analysis reveals that no study reports AUC, sensitivity, and specificity alongside an explicit differential privacy budget (ε), a critical gap for clinical deployment. We propose a four-component framework-compressed client models, tunable differential privacy, lightweight integrity protection, and hardware-realistic validation-supported by a pseudocode algorithm and architecture diagram. Eight research gaps are identified, with client-side model compression and standardised privacy–utility reporting identified as the highest priorities.

Keywords - Federated Learning; Remote Patient Monitoring; IoHT; Lightweight Edge AI; Differential Privacy; Privacy–Accuracy Trade-off; PRISMA; Systematic Review.

I. INTRODUCTION

The Internet of Healthcare Things (IoHT) has transformed remote patient monitoring (RPM) from episodic clinic visits into a continuous, data-intensive discipline. Wearable sensors and implanted devices now generate cardiac rhythms, blood glucose, blood pressure, and EEG signals at unprecedented scale [1]. This physiological stream enables predictive analytics for early detection of cardiac events, sepsis, and chronic disease deterioration, yet simultaneously concentrates highly sensitive data subject to HIPAA and GDPR [18].

The conventional centralised approach-aggregating raw patient data on a cloud server-introduces two structural problems: (i) transferring raw physiology off-device expands the attack surface and triggers regulatory requirements [2, 3]; and (ii) cloud round-trip latency is incompatible with real-time RPM services such as arrhythmia detection [5].

Federated learning (FL), introduced by McMahan et al. [29], enables multiple distributed clients to train a shared model by exchanging only model updates, never raw data [6, 7]. Foundational advances established formal convergence guarantees [30], healthcare applicability [31], and characterised heterogeneous-hardware challenges [32]. However, the healthcare FL literature has prioritised accuracy and privacy over deployability on constrained hardware. Many reviewed frameworks run client computation on cloud-hosted simulators rather than physical wearables [8, 9].

This review covers 2022–2026 because lightweight IoHT-specific FL-applying model compression, quantisation, and on-device training to wearable hardware-only emerged as a systematic research focus after 2021. Earlier foundational work is covered by [29–32]; the present review explicitly characterises itself as a survey of recent developments.

A. Definition of "Lightweight"

To resolve terminological ambiguity across the corpus, we adopt a three-dimensional operational definition. A FL framework is classified as lightweight only if it reduces resource demands on one or more of: (MS) Client model size-parameter count or storage footprint reduced via pruning, quantisation, or distillation; (CC) Communication cost-gradient volume per round reduced via compression or sparsification; (EC) Device energy consumption-measurable energy reduction measured on physical constrained

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

hardware. Frameworks achieving efficiency solely by offloading computation to a fog or cloud server do NOT qualify as lightweight under this definition, as the client-resident model is unchanged. Table III scores all ten representative frameworks against MS, CC, and EC explicitly.

II. LITERATURE REVIEW METHODOLOGY

A. Search Strategy

Records were retrieved from multiple open-access bibliographic repositories using the query "Lightweight Federated Learning Framework for Privacy-Preserving Predictive Analytics in Remote Patient Monitoring (IoHT)", restricted to 2022–2026. This returned 257 records spanning IEEE, Springer, MDPI, Elsevier, Nature, and arXiv. The search was conducted in accordance with PRISMA 2020 guidelines [33].

TABLE I
SEARCH CORPUS COMPOSITION

Attribute	Value	Notes
Database	Multiple open-access journals	IEEE, Springer, MDPI, Elsevier, Nature, arXiv
Records retrieved	257	Open access only, 2022–2026
Year range	2022–2026	87 records in 2025 (rapid growth)
Top venues	IEEE Access; Scientific Reports; arXiv	Mix of conference and journal

B. Screening and Eligibility

After removing 3 duplicates, 254 unique records were screened at title-and-abstract level against two inclusion criteria: (i) explicit treatment of federated, collaborative, or decentralised learning; and (ii) explicit relevance to health, clinical, or IoHT/IoMT contexts. Records failing either criterion were excluded (n = 222). Full-text review of the remaining 32 records excluded 4 further entries (front-matter or off-topic). The final synthesis corpus comprised 28 studies. The PRISMA 2020 screening flow is shown in Fig. 1.

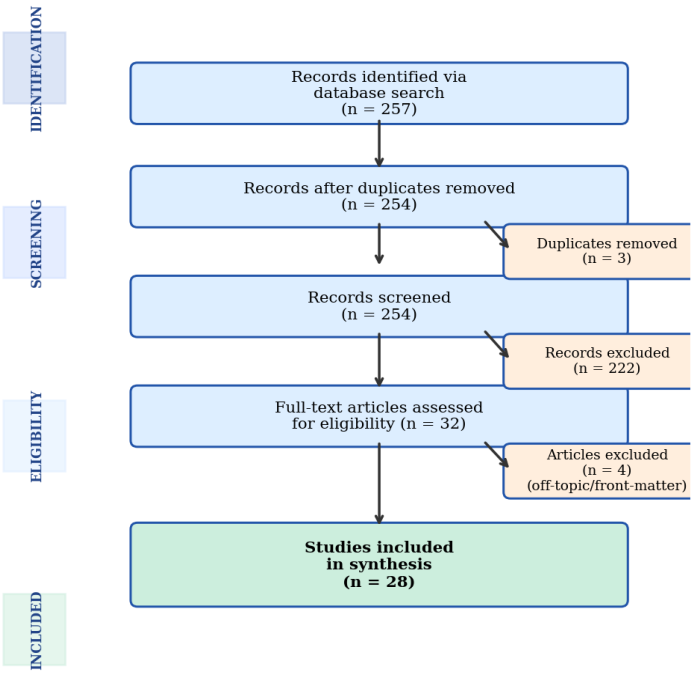

Fig. 1. PRISMA 2020 Study Selection Flow Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

III. RESULTS AND DISCUSSION

A. Publication Trend

The 28 included studies are concentrated in 2025–2026: 1 (2022), 4 (2023), 4 (2024), 14 (2025), 5 (2026) as shown in Fig. 2. Nineteen of 28 studies (68%) were published in 2025–2026, confirming that lightweight IoHT-specific FL is a rapidly accelerating research focus and validating the 2022–2026 scope.

Fig. 2. Year-wise Distribution of Included Studies (2022-2026)

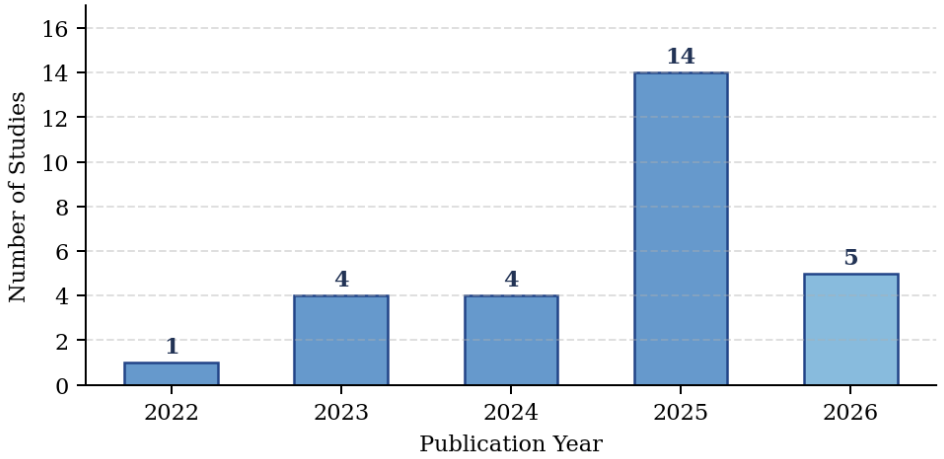

Fig. 2. Year-wise distribution of included studies (2022–2026).

B. Thematic Taxonomy

Thematic analysis identified five clusters (Table II, Fig. 3): blockchain–federated integration, FL-based security and intrusion detection, privacy-preservation techniques, lightweight and edge-efficient architectures, and general FL/IoHT surveys. Each cluster contains five or six studies, indicating broadly distributed research attention.

TABLE II
THEMATIC AND METHODOLOGICAL TAXONOMY

Thematic Cluster	Research Focus	Key Studies	Methodological Emphasis
Blockchain–FL Integration	Decentralised trust and incentive layers with FL	[3],[7],[9],[10],[11]	Consensus protocols, smart contracts
FL-Based Security & IDS	FL to detect poisoning, inference, network attacks	[12],[13],[14],[15],[16]	Federated classifiers, graph learning
Privacy-Preservation	DP, secure aggregation, robust aggregation	[2],[17],[18],[19],[20]	Formal privacy guarantees, robustness
Lightweight / Edge	Fog/edge offloading, lightweight authentication	[5],[8],[21],[22],[23],[24]	Edge computation, lightweight protocols
General FL/IoHT Surveys	Broad FL application and IoHT convergence surveys	[1],[6],[25],[26],[27],[28]	Narrative and systematic survey methods

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

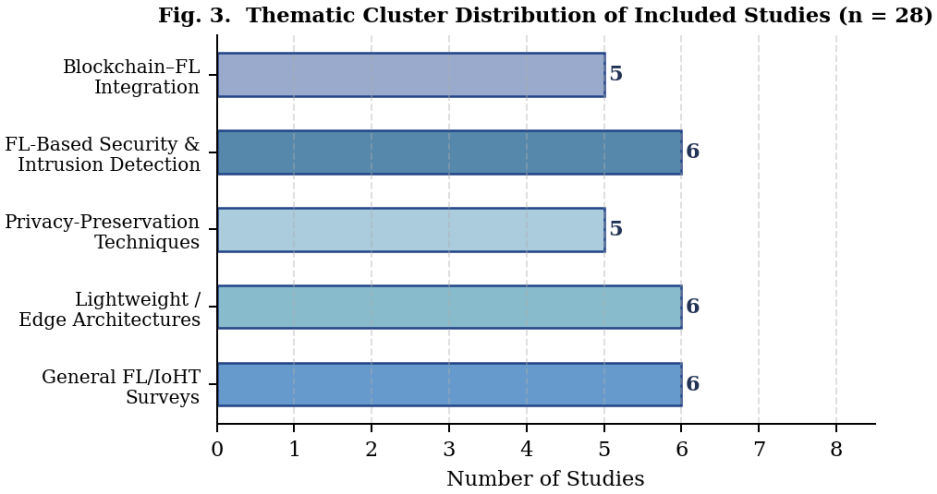

Fig. 3. Thematic cluster distribution of included studies (n = 28).

C. Comparative Framework Analysis

Ten representative frameworks were compared across privacy mechanism, efficiency strategy, lightweight criteria (MS/CC/EC), validation dataset, and key limitation (Table III). Validation data type: R = real clinical; Sy = synthetic; Si = simulation; N = no validation.

TABLE III
COMPARATIVE EVALUATION OF TEN REPRESENTATIVE FL FRAMEWORKS

Ref.	Framework Focus	Privacy Mechanism	Lightweight Strategy	MS	CC	EC	Validation Dataset	Type	Key Limitation
[21]	Edge-based secure health monitoring	Edge encryption before cloud	Fog layer offloading	x	x	x	Simulated edge-node scenarios	Si	No client-model compression
[3]	Blockchain-RL FL for IoMT (COVID-19)	Blockchain-anchored updates; RL	Distributed computation	x	P	x	COVID-19 dataset (simulated partition)	R/Si	Consensus scalability not benchmarked
[5]	Hybrid fog-edge for real-time monitoring	Localised processing	Fog layer latency reduction	x	x	x	Synthetic IoMT traffic data	Sy	Fog vs. latency trade-off unquantified
[8]	Hybrid federated SVM + trust management	Trust-score-gated participation	Lightweight SVM; power objective	P	P	P	Simulation; no clinical dataset	Si	No physical hardware energy measure
[22]	Lightweight authentication for IoMT	Auth. protocol limits ID exposure	WBAN communication overhead minimised	x	Y	x	Synthetic WBAN scenario data	Sy	Isolated from FL training pipeline
[10]	Blockchain-enhanced FL (survey)	DP + blockchain aggregation (survey)	Not benchmarked	x	x	x	No empirical evaluation	N	Survey only; no empirical framework
[2]	FED-EHR decentralised analytics	Federated training; no noise injection	Wearable-sensor targets; no compression	x	x	x	Real EHR-linked wearable sensor data	R	Lightweight not a primary objective

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

[9]	Adaptive blockchain + RL consensus	Blockchain update integrity	RL-based resource forecasting	x	P	x	Simulated IoMT network	Si	Evaluated on simulation not hardware
[24]	CNN-GRU + differential privacy	DP on federated aggregation step	CNN-GRU sized for telemedicine	P	P	x	PhysioNet MIT-BIH; MIMIC-III	R	e-value not stated; no energy measure
[11]	Quantum-enhanced federated blockchain	Multi-chain + adaptive consensus	Dynamic relational learning	x	x	x	Multi-modal cardiovascular data	R	Quantum overhead not characterised

MS = model size reduction; CC = communication cost reduction; EC = energy consumption reduction. Y = fully addressed; P = partial; x = not addressed.

D. Privacy–Accuracy Trade-off Analysis

Table IV and Fig. 4 consolidate privacy–accuracy reporting across all 28 studies. Key findings: (i) only [24] reports any diagnostic accuracy alongside a DP mechanism, and even there the ε value is not stated; (ii) no study reports AUC, sensitivity, and specificity jointly with an explicit ε; (iii) most privacy mechanisms (blockchain, trust-gating, secure aggregation) have no tunable ε, making cross-study comparison impossible.

Fig. 4. Privacy-Accuracy Reporting Gap Across 28 Included Studies

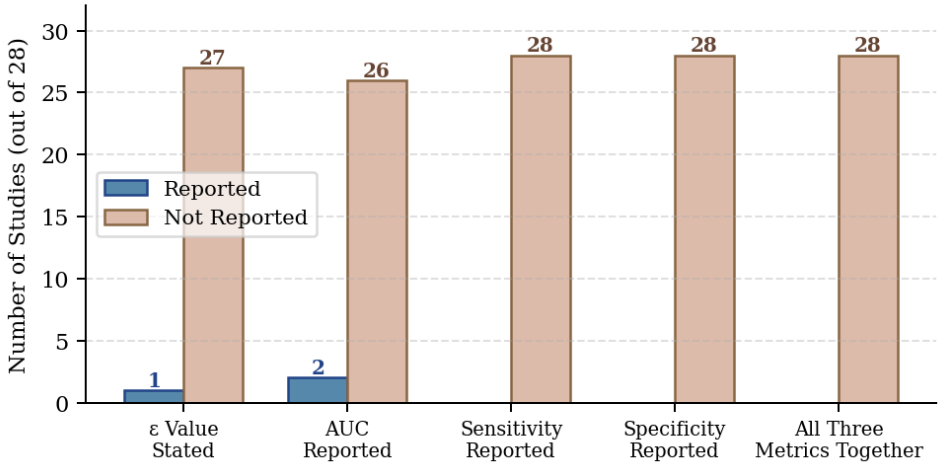

Fig. 4. Privacy–accuracy reporting gap across 28 included studies.

TABLE IV
PRIVACY–ACCURACY TRADE-OFF SUMMARY (SELECTED STUDIES)

Ref.	Privacy Mechanism	e Value	AUC	Sensitivity	Specificity	Overall Acc.	Status
[24]	DP on CNN-GRU aggregation	NR	NR	NR	NR	~95% (1 pt)	Incomplete: e and full metrics missing
[2]	Federated training (no DP)	N/A	NR	NR	NR	NR	Gap: no clinical accuracy reported
[8]	Trust-score gating (non-DP)	N/A	NR	NR	NR	Power metrics only	Gap: no clinical accuracy
[3]	Blockchain RL (no DP)	N/A	NR	NR	NR	Risk score only	Gap: no accuracy metrics
[17]	DP survey (conceptual)	Multiple	NR	NR	NR	NR	Conceptual only

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

[10]	DP + blockchain (survey)	NR	NR	NR	NR	NR	Conceptual only
[12]-[16]	FL intrusion detection	N/A	Detection AUC	NR	NR	Detection accuracy	Not clinical diagnostic accuracy

Recommended reporting protocol: Future studies should state (a) explicit ε value; (b) AUC, sensitivity, specificity; (c) metrics at ε ∈{0.1, 1.0, 10.0}; (d) noise scale σ calibration method.

IV. SUMMARY FINDINGS

TABLE V
STRENGTHS AND WEAKNESSES ACROSS THE REVIEWED CORPUS

ID	Theme	Finding
S1	Privacy-mechanism diversity	DP, secure aggregation, blockchain, and trust-gating each independently validated across multiple studies [8,10,17,19,20].
S2	Rapid growth	14 of 28 studies (50%) published in 2025 alone; field is accelerating.
S3	Cross-domain base	Corpus spans federated optimisation, blockchain, CNN-GRU, and lightweight cryptography [22,24].
S4	Clinical validation (subset)	[24] uses PhysioNet MIT-BIH and MIMIC-III; [2] uses real EHR data.
W1	Lightweight inconsistency	7 of 10 frameworks score (MS x, CC x, EC x)-efficiency via offloading only (Table III).
W2	No hardware energy benchmarking	No study measures EC on physical microcontroller or wearable hardware.
W3	Privacy–utility unreported	Only [24] links accuracy to DP; no study reports AUC/Sens/Spec with stated ε (Table IV).
W4	Blockchain overhead uncharacterised	No study reports latency, energy, or bandwidth added by consensus on constrained clients [3,9,11].
W5	Fragmentation	Authentication [22], IDS [13,15], aggregation [19] addressed in isolation, not integrated.

V. RESEARCH GAP ANALYSIS

TABLE VI
RESEARCH GAP ANALYSIS

Dimension	Gap Description	Evidence	Severity
Model efficiency	No study benchmarks model compression on physical constrained IoHT hardware using MS/CC/EC criteria	[8],[22],[9],[24]	Critical
Validation realism	Most use simulated or single-domain datasets; see Table III validation column	[2],[24],[11]	Critical
Privacy–utility trade-off	No study reports AUC, Sens., Spec. across multiple ε values (Table IV)	[17],[19],[24]	Critical
Overhead accounting	Blockchain consensus/IDS not benchmarked for energy, latency, bandwidth on constrained clients	[3],[13],[9]	High
Integration	Auth., IDS, aggregation, and lightweight design treated as isolated sub-problems	[19],[22],[16]	High
Standardisation	No shared benchmark suite or resource-cost reporting format for RPM FL comparison	All 28 studies	High
Adaptive client mgmt.	Client selection and personalisation for heterogeneous wearables underexplored	[26],[8]	Moderate
Regulatory alignment	Few studies map privacy mechanisms onto HIPAA or GDPR requirements	[18],[20]	Moderate

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

VI. PROPOSED LIGHTWEIGHT FRAMEWORK

A. Architecture Overview

Drawing on the gap analysis, a practically deployable framework requires four components currently appearing in isolation across the corpus (Fig. 5): (1) Compressed client models-INT8 quantised or pruned architectures sized for wearable hardware; (2) Tunable differential privacy-calibrated noise with explicit ε and accuracy reporting at multiple budget levels; (3) Lightweight integrity protection-trust-score gating without full blockchain consensus overhead; (4) Realistic hardware validation-energy and latency benchmarking on physical constrained platforms using PhysioNet MIT-BIH or MIMIC-III.

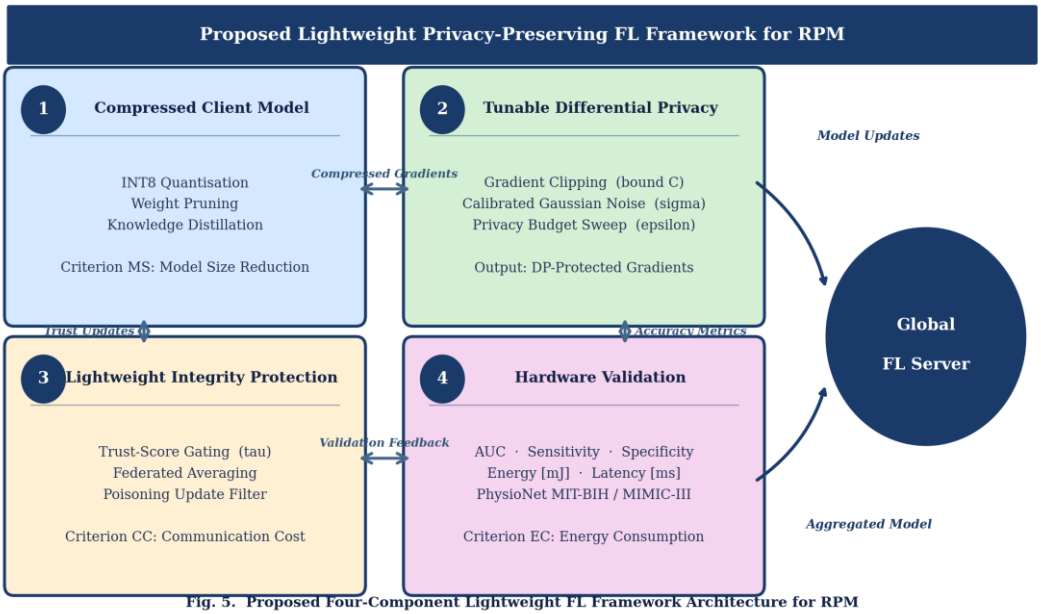

Fig. 5. Proposed Four-Component Lightweight FL Framework Architecture for RPM

B. Algorithm

Algorithm 1 presents pseudocode showing how all four components interact within one training round, making their data-flow dependencies explicit for the first time in this corpus. The compressed model (C1) determines gradient magnitude that DP (C2) must clip and perturb. Trust-score gating (C3) filters the resulting DP-gradients. Validation (C4) evaluates AUC/sensitivity/specificity per round on a standardised clinical dataset, closing the privacy–accuracy feedback loop.

Algorithm 1: Lightweight Privacy-Preserving Federated Learning for Remote Patient Monitoring (RPM)

Input:

N : Number of clients
M0 : Initial compressed global model
ε, δ, C : Differential Privacy parameters
r : Compression ratio
θ : Trust threshold
T : Number of communication rounds
E : Number of local training epochs

Output:

MT : Trained lightweight global model

Initialize

1. Compute DP noise scale:

$\sigma \leftarrow C \times \sqrt{(2 \times \ln(1.25 / \delta))} / \varepsilon$

2. Initialize trust score for each client:

$\tau_i \leftarrow 0.5$ for i = 1 to N

3. Deploy compressed model M0 to all clients.

For each communication round t = 1 to T do

Server (Integrity Module)

4. Select trusted clients:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

$St \leftarrow \{ i \mid \tau i \geq \theta \}$

5. Broadcast global model M(t−1) to all clients in St.

Client-Side Training (Compressed Model)

6. For each client $i \in St$ do

Load compressed model M(t−1).

Train locally using SGD for E epochs:

$Mi(t) \leftarrow LocalSGD(M(t-1), Di, E)$

Compute local update:

$\Delta Mi \leftarrow Mi(t) - M(t-1)$

Client-Side Differential Privacy

7. Clip the model update:

$\Delta Mi \leftarrow \Delta Mi \times \min(1, C / \|\Delta Mi\|)$

8. Add Gaussian noise:

$\Delta MiDP \leftarrow \Delta Mi + N(0, \sigma^2 C^2 I)$

9. Send ΔMiDP to the server.

10. Log client resource usage:

Energy Ei (mJ)

Latency Li (ms)

Server Aggregation and Integrity Verification

11. Update trust score:

$\tau i \leftarrow TrustUpdate(\tau i, \Delta MiDP)$

12. Re-filter trusted clients:

$St^* \leftarrow \{ i \mid \tau i \geq \theta \}$

13. Aggregate model updates:

$Mt \leftarrow M(t-1) + (1 / |St^*|) \times \Sigma \Delta MiDP$

14. Requantize Mt to maintain compressed representation.

Model Validation

15. Evaluate Mt on PhysioNet / MIMIC-III holdout dataset.

6. Report:

- AUC
- Sensitivity
- Specificity
- Average Energy Consumption (mJ)

End For

Return

17. Return final global model MT.

VII. FUTURE WORK

Four priority directions emerge from Table VI. First, hardware-realistic benchmarking on physical microcontroller-class platforms (e.g., ARM Cortex-M) with standardised energy and latency measurement must accompany every future accuracy result. Second, privacy–utility curves reporting AUC, sensitivity, and specificity at $\varepsilon \in \{0.1, 1.0, 10.0\}$ should become the community standard for DP-enhanced RPM frameworks. Third, a unified benchmark suite-combining non-IID splits of PhysioNet MIT-BIH or MIMIC-III with a defined resource-cost reporting format-would enable the first reproducible cross-study comparison. Fourth, adaptive client selection and personalisation strategies for heterogeneous wearable fleets warrant investigation, extending the trust-management work of [8] to hardware-realistic settings.

VIII. CONCLUSION

This systematic review synthesised 28 studies (2022–2026) on lightweight, privacy-preserving FL for remote patient monitoring. A formal three-dimensional lightweight definition (MS, CC, EC) applied to Table III reveals that 7 of 10 representative frameworks achieve efficiency only through network offloading, satisfying none of the three criteria. A new privacy–accuracy trade-off analysis shows that no study reports AUC, sensitivity, and specificity alongside an explicit ε, identifying a critical gap for clinical deployment. The proposed four-component architecture (Fig. 5, Algorithm 1) integrates compressed client models, tunable

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

differential privacy, lightweight integrity protection, and hardware-realistic validation in a single measured pipeline-a configuration no reviewed study implements end-to-end. Implementing and benchmarking this pipeline on physical constrained hardware against PhysioNet MIT-BIH and MIMIC-III is identified as the field's most impactful next step.

.REFERENCES

[1] P. He, D. Huang, D. Wu et al., "A survey of Internet of medical things: technology, application and future directions," Digital Commun. Netw., vol. 12, no. 5, pp. 717–742, 2026.
[2] R. U. Z. Wani and O. Can, "FED-EHR: A Privacy-Preserving Federated Learning Framework for Decentralized Healthcare Analytics," Electronics, vol. 14, no. 16, pp. 3261, 2025.
[3] C. Dhasaratha, M. K. Hasan, S. Islam et al., "Data privacy model using blockchain reinforcement federated learning for scalable IoMT," CAAI Trans. Intell. Technol., 2024.
[4] S. Punitha and K. S. Preetha, "Enhancing reliability and security in cloud-based telesurgery using swarm-evoked distributed FL," Sci. Rep., vol. 15, pp. 27226, 2025.
[5] U. Islam et al., "A hybrid fog-edge computing architecture for real-time health monitoring in IoMT," Sci. Rep., vol. 15, pp. 25655, 2025.
[6] D. Sirohi et al., "Federated learning for 6G-enabled secure communication systems: a comprehensive survey," Artif. Intell. Rev., vol. 56, pp. 11297–11389, 2023.
[7] N. Nezhadsistani, N. S. Moayedian, and B. Stiller, "Blockchain-Enabled Federated Learning in Healthcare: Survey and State-of-the-Art," IEEE Access, vol. 13, pp. 119922–119945, 2025.
[8] S. Khan et al., "An Expert Hybrid Federated Learning and Trust Management for Security, Efficiency, and Power Optimization in Smart Health," IEEE Access, vol. 13, pp. 58191–58210, 2025.
[9] C. V. N. U. B. Murthy and M. L. Shri, "An Adaptive Blockchain Framework for Federated IoMT with RL-Based Consensus," Sci. Rep., vol. 16, pp. 8296, 2026.
[10] Z. N. Limbepe, K. Gai, and J. Yu, "Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey," Blockchains, vol. 3, no. 1, pp. 1, 2025.
[11] R. Sivakami et al., "Quantum-enhanced federated blockchain for privacy-preserving cardiovascular intelligence," Sci. Rep., 2026.
[12] S. A. Alzakari et al., "Converging Technologies for Health Prediction and Intrusion Detection in IoHT," IEEE Access, vol. 12, pp. 99469–99498, 2024.
[13] R. Bensaid et al., "SA-FLIDS: Secure and Authenticated FL-Based Intelligent Network IDS for Smart Healthcare," PeerJ Comput. Sci., vol. 10, e2414, 2024.
[14] S. R. Hassan et al., "A comprehensive survey on intrusion detection in IoMT," ICT Express, vol. 11, no. 6, pp. 1291–1310, 2025.
[15] F. S. Alrayes et al., "Hybrid Cross-Temporal Contrastive Model with Spiking Energy-Efficient IDS in IOMT," Int. J. Comput. Intell. Syst., vol. 18, pp. 270, 2025.
[16] A. Daulay et al., "Novel Federated Graph Contrastive Learning for IoMT Security," Mathematics, vol. 13, pp. 2471, 2025.
[17] X. Gu, F. Sabrina, Z. Fan, and S. Sohail, "A Review of Privacy Enhancement Methods for FL in Healthcare," Int. J. Environ. Res. Public Health, vol. 20, pp. 6539, 2023.
[18] N. Khalid et al., "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," Comput. Biol. Med., vol. 158, pp. 106848, 2023.
[19] M. Aggarwal et al., "A Survey on Privacy-Preserving Healthcare Services Focusing on Robust Aggregation," Int. J. Comput. Intell. Syst., vol. 18, pp. 326, 2025.
[20] K. Li et al., "Privacy preservation in blockchain-based healthcare data sharing," Peer-to-Peer Netw. Appl., vol. 18, pp. 302, 2025.
[21] A. Singh and K. Chatterjee, "Edge computing based secure health monitoring framework for electronic healthcare," Cluster Comput., vol. 26, pp. 1205–1220, 2022.
[22] A. Merchant et al., "An efficient lightweight authentication scheme for smart healthcare in IoMT," Discov. Comput., vol. 28, pp. 261, 2025.
[23] Y. Chen and C. Lin, "Application of Edge Computing IoT Architecture in Community Care Service Systems," Eng. Technol. J., vol. 10, pp. 5668–5683, 2025.
[24] N. Naik et al., "Design and optimisation of an IoT-based AI framework for real-time health monitoring and telemedicine diagnostics," Discov. Internet Things, vol. 6, pp. 37, 2026.
[25] R. Ahmad et al., "Digital-care in next generation networks: Requirements and future directions," Comput. Netw., vol. 224, pp. 109599, 2023.
[26] E. Zeydan, S. S. Arslan, and M. Liyanage, "Managing Distributed ML Lifecycle for Healthcare Data in the Cloud," IEEE Access, vol. 12, pp. 115750–115774, 2024.
[27] "Federated Learning Applications in the Industrial Internet of Everything (IoE)," Stud. Syst. Decis. Control, vol. 611, 2025.
[28] "The Convergence of Federated Learning and Healthcare 5.0 and Beyond," Stud. Comput. Intell., vol. 1247, 2026.
[29] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," Proc. AISTATS, vol. 54, pp. 1273–1282, 2017.
[30] P. Kairouz et al., "Advances and Open Problems in Federated Learning," Found. Trends Mach. Learn., vol. 14, no. 1–2, pp. 1–210, 2021.
[31] N. Rieke et al., "The future of digital health with federated learning," NPJ Digit. Med., vol. 3, pp. 119, 2020.
[32] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, 2020.
[33] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, pp. n71, 2021.