Secure Federated Learning Frameworks for ECG Analysis: A Comprehensive Review

[1]Sukhwinder Kaur, [2]Er.Simarjot Kaur, [3]Er.Shabad Kaur
[1]M. Tech Scholar, Department of CSE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India
[2]Assistant Professor, Department of CSE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India
[3]Assistant Professor, Department of CSE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India

Abstract : The rapid expansion of digital healthcare and the Internet of Medical Things technologies has significantly enhanced the need for privacy preserving analytics in ECG based cardiac monitoring systems. Federated Learning has come up as a promising paradigm that lets multiple healthcare institutions train together, across distributed sites, without exchanging raw patient data. This review gives a comprehensive analysis of the existing research on secure federated learning approaches for ECG signal processing. The study looks at commonly used datasets, different signal pre-processing strategies, deep learning architectures including LSTM based models, federated optimization algorithms, and a set of privacy enhancing methods like Differential Privacy, homomorphic encryption, and also secure aggregation.

A critical methodological assessment highlights some key challenges including privacy–performance trade-offs, statistical heterogeneity across distributed client's communication overhead, plus computational constraints and also security vulnerabilities in federated settings. The review also seems to point out scalability limitations when people try to use it in real-world healthcare deployments and that there is a limited emphasis on time-series forecasting compared to classification tasks. So, based on these findings, the study argues for a specialized privacy-preserving federated LSTM framework that is tailored for ECG time-series analysis. In the end, future research should focus on communication-efficient aggregation, adaptive privacy calibration, and resilience to adversarial attacks, and then also push for large-scale multi-institutional validation so it can support secure scalable and clinically dependable federated cardiac monitoring systems.

Index Terms **- Federated Learning, ECG Signal Analysis, Privacy-Preserving Healthcare, LSTM Networks, Internet of Medical Things (IoMT)**

1.INTRODUCTION

The rapid growth of wearable sensors, remote patient monitoring setups, and intelligent healthcare platforms has sort of really changed cardiac data analytics quite a bit, electrocardiogram signals (ECG) plus heart-rate time-series streams delivers essential clues for early detection of arrhythmias, heart failure, and other cardiovascular issues. At the same time, there are more apprehensions about data secrecy and regulatory compliance which have basically constrained centralized data sharing between hospitals and institutions. Lately, advances in deep learning and distributed model training, have opened up new pathways for building secure, scalable, privacy-preserving cardiac analysis frameworks. This review is centered on how Long Short-Term Memory networks are integrated with federated learning paradigms so that ECG time-series analysis stays accurate while remaining protected and secure.

1.1 Background of ECG and Heart-Rate Time-Series Analysis

ECG signals are really showing the electrical activity of the heart and they are kind of sequential by nature. For an accurate readout, model temporal dependencies, the shape of the waveform, and also the differences that show up from beat to beat. Usual statistical

techniques or rule based methods often have a hard time with the tangled non linear patterns that appear in cardiac signals. More recently, deep learning methods, especially mixed CNN–LSTM architectures, have shown better performance for automated diagnosis jobs like congestive heart failure detection, because they manage to capture both spatial cues and time related cues from ECG recordings [1].

For an accurate readout, you have to somehow model temporal dependencies, the shape of the waveform, and also the differences that show up from beat to beat.

1.2 Role of Deep Learning in Cardiac Signal Processing

Deep learning has significantly modified the cardiac signal processing by supporting automated feature extraction and better pattern recognition on ECG records. In contrast to older machine learning approaches that lean on handcrafted descriptors, deep neural networks can learn layered, more natural representations straight from the raw signals. Convolutional Neural Networks (CNNs) do well at picking up local morphological traits of ECG waveforms, and then Recurrent Neural Networks (RNNs), including their offshoots, tend to track temporal relationships across cardiac cycles [3]. Between these options, LSTM and GRU networks are often a fit for time-series healthcare data because they reduce vanishing gradient issues and they keep longer term contextual cues.

When you compare the recurrent setups, results often suggest that LSTM models tend to train more steadily on long sequences of physiological data, while GRU models are lighter and run faster since they use fewer parameters [4]. In cardiac signal processing, where you need both high accuracy and real-world computational feasibility,the choice between LSTM and GRU usually comes down to factors like dataset size, signal duration, and deployment limits. Altogether, these observations position LSTM driven architectures as a solid groundwork for ECG time-series modeling especially when they are paired with privacy-preserving distributed learning strategies.

1.3 Privacy Challenges in Healthcare Data

Confidentiality of Electronic Health Records (EHRs): Digital health records keep a lot of very sensitive clinical and personal stuff, so they become kind of easy targets for unauthorized access and misuse [5]. Keeping strict confidentiality is really important , to make sure patients still trust you and to meet regulatory compliance, even if it sounds basic.

Complex access control and data sharing policies: Healthcare data usually touches a bunch of stakeholders, like hospitals, insurers, and researchers. Trying to manage controlled access while still allowing collaborative analytics is a lot more complicated than it appears, because governance decisions don't stay in one place.

Risk of transitive information leakage: Even if direct identifiers are removed, sensitive details can sometimes be inferred using linked systems or by looking at aggregated outputs [6]. That indirect leakage isn't minor, it can seriously threaten interconnected healthcare infrastructures where everything connects.

Inference attacks in analytical systems: Modern data analytics models can accidentally expose private attributes, for example through prediction outputs or even model updates. These risks tend to get worse when models are trained on distributed medical datasets, because the training process itself can "remember" patterns.

Regulatory and ethical compliance constraints: Using healthcare data has to follow strict privacy regulations plus ethical guidelines. And balancing innovation in AI-driven diagnostics with legal obligations is still a persistent challenge [5].

1.4 Emergence of Federated Learning

Federated Learning (FL) enables collaborative model training without transferring raw data to a centralized server. Instead of collecting whole datasets, FL does model update aggregation. so the system can lower the direct visibility of sensitive information, at least in principle [7]. This decentralized way of training is often a fit for healthcare settings because patient records are usually spread across hospitals, laboratories, and even wearable devices, quite literally everywhere.

Broader surveys report that FL can boost data privacy, offer better scalability, and align more easily with regulatory boundaries, yet still keep model quality fairly competitive [7]. In smart healthcare frameworks, FL can be used for cross-institutional analytics, for

remote monitoring of patients, and for IoMT-driven processing, all while trying not to break confidentiality promises [8]. Still, there are issues that keep showing up, like communication overhead, statistical heterogeneity, and security risks. So even though the benefits are clear, these topics remain hot research targets, especially when the medical signals are time series and the timing matters.

1.5 Motivation and Scope Toward Privacy-Preserving Federated LSTM Framework

Recent studies show that LSTM based models can be merged with privacy protecting mechanisms to let secure heart rate estimation happen in distributed settings [9]. In practice, these ideas suggest that good sequential modeling and privacy protection aren't really opposites, especially when verification steps and secure aggregation approaches are woven into the training routine.

Differential privacy has been suggested as a more formal method for shielding sensitive data while the model is being trained, basically by injecting carefully controlled noise into gradients or parameters [10]. When it is combined with federated learning, differential privacy tends to improve the model's resistance to inference and reconstruction attacks. Taking these developments into account, this review is aimed at surveying current work across LSTM based ECG modeling, federated learning and privacy preserving mechanisms to determine what limitations still exist and what future research avenues.

2. Literature Review

Recent advancements in intelligent health care systems have sped up the way deep learning and distributed computing are being merged for medical data analytics. In particular, ECG and heart rate time-series analysis has gained a lot from sequential deep learning architectures, plus privacy aware training tricks that are trying to stay compliant. As worries keep growing about where the data lives, like centralized storage, and also about regulatory compliance, researchers have started looking into federated learning, differential privacy, blockchain integration, and also mixed cryptographic mechanisms. The idea is to make sure institutions can train models together, but in a secure and controlled way, even when data cannot be directly shared.

Overall , the literature is pointing toward a more privacy preserving direction, where instead of one centralized deep learning model, researchers move toward federated frameworks that are made for healthcare use. Newer works often stress multimodal ECG classification, IoMT style monitoring, secure sensor data fusion, and analytics that span across different institutions. Still there are differences left, especially in architectural design , the exact privacy mechanisms, how well scalability is evaluated, and how applicable these methods are to sequential LSTM based

Table 1: Comparative Analysis of Privacy-Preserving Federated Learning Approaches in Healthcare

Author / Year	Learning Model / Architecture	Privacy Technique	Key Contribution	Limitations / Research Gap
Marrah et al., 2026	Federated Deep Learning	Secure FL aggregation	Distributed deep learning for healthcare analytics	Limited ECG-specific sequential modeling focus
Huan et al., 2026	FedMCF-xLSTM (Federated xLSTM)	Federated contrastive learning	Multimodal multi-label ECG classification using federated xLSTM	High computational complexity and communication cost
Senthuran et al., 2025	Deep learning ECG framework	Privacy-aware framework	Secure ECG analysis in immersive healthcare environments	Lacks full federated scalability validation

Wani & Can, 2025	Federated EHR analytics	Privacy-preserving FL	Decentralized healthcare analytics using FL	Not focused on time-series ECG modeling
Almogadwy & Alqarafi, 2025	Fused Federated Learning	Secure IoMT-based FL	Decentralized patient monitoring in Healthcare 5.0	Limited evaluation on sequential ECG datasets
Shi, 2025	Federated Learning Framework	Differential Privacy + Homomorphic Encryption	Multi-institution secure healthcare analytics	Increased computational overhead
Wang et al., 2025	Multimodal Federated Learning	Privacy-preserving FL	Secure multi-modal sensor data fusion	ECG-specific LSTM modeling not deeply explored
Ghazarian et al., 2024	ECG data analysis models	Differential Privacy	DP-based ECG privacy study with case analysis	No federated implementation
Goranthala et al., 2024	Federated IoT-based arrhythmia detection	Secure FL aggregation	Privacy-preserving arrhythmia detection	Limited scalability analysis
Lakhan et al., 2024	Deep Federated Learning	Secure distributed learning	Healthcare framework using deep FL schemes	No explicit differential privacy mechanism
Alsamhi et al., 2024	Blockchain + Federated Learning	Blockchain-based privacy	Decentralized healthcare data sharing	Communication latency issues
Yazdinejad et al., 2024	Hybrid Federated Learning	Hybrid privacy-preserving FL	Robust FL against irregular users	Not tailored to ECG time-series modeling
Kumar et al., 2024	Blockchain-based Federated Learning	Blockchain privacy integration	Secure medical image segmentation	Focused on imaging, not ECG signals
Ogbuabor, 2023	Context-aware cardiac framework	Privacy-preserving architecture	Secure cardiac health monitoring system	No federated training validation
Yazdinejad et al., 2023	AP2FL Framework	Auditable Privacy-Preserving FL	Auditable and secure FL system	Limited real-world ECG evaluation
Dasaradharami & Gadekallu, 2023	FL Survey	General privacy mechanisms	Comprehensive survey of FL in healthcare	Lacks technical implementation insights

Oh & Nadkarni, 2023	Federated structured data learning	Secure FL	FL for structured medical datasets	Limited focus on deep sequential models
Aziz et al., 2023	Federated Learning	Homomorphic Encryption + DP	Secure FL paradigm using HE and DP	Computationally intensive
Shen et al., 2023	FL with DP simulations	Differential Privacy	Privacy-utility trade-off analysis	Simulation-based, limited clinical validation
Sun & Wu, 2022	Scalable Federated Learning	Secure FL	Transferable FL for healthcare sensor data	Not ECG-specific
Akter et al., 2022	Edge-based Federated Learning	Privacy-preserving FL	Edge intelligence healthcare framework	No LSTM-specific modeling
Singh et al., 2022	FL + Blockchain	Blockchain-based privacy	IoT healthcare data protection	Increased communication overhead
Wang et al., 2022	Federated IoMT learning	Privacy-preserving FL	Secure FL under edge computing	Limited sequential deep learning focus
Vizitiu et al., 2021	Wearable health deep learning	Privacy-preserving framework	Atrial fibrillation detection framework	Not fully federated
Li et al., 2021	Federated Learning Systems Survey	Privacy-preserving FL	Comprehensive FL system survey	Broad scope, lacks ECG specialization

3.Research Methodology Analysis in Existing Studies

This section critically looks at how methodological choices are made in existing privacy preserving federated learning work for ECG and healthcare time series analytics. The discussion basically ties together previous research to spot dominant design patterns, various implementation strategies, and methodological gaps that matter for federated LSTM, based cardiac monitoring systems.

3.1 Commonly Used Datasets

Existing studies tap into a mix of publicly available ECG repositories, in-house clinical datasets, and IoMT sensor streams to test federated healthcare frameworks. The ECG–heavy line of work tends to lean on curated cardiac datasets, which are used to check arrhythmia detection and classification accuracy (Senthuran et al., 2025). When people build multimodal federated ECG systems,

they often try to mimic how decentralized hospitals behave, using distributed datasets that stand in for real-world cross- institution collaboration (Huan et al., 2026).

More general federated healthcare frameworks also pull together Electronic Health Records alongside heterogeneous sensor data gathered from decentralized clinical settings (Wani and Can, 2025; Lakhan et al., 2024). Even so, while those datasets can improve generalizability, there are still issues: mismatched or uneven data partitioning plans, and not enough emphasis on statistical heterogeneity, which then makes results harder to compare. Also, only a few works tackle non-IID ECG time-series patterns across federated clients in a systematic way. Those patterns, in practice, can strongly sway model convergence as well as end performance.

3.2 Signal Preprocessing Techniques

Common preprocessing strategies applied in reviewed studies include:

a) Noise filtering and baseline wander removal to improve ECG signal quality (Ghazarian et al., 2024).
b) Segmentation of cardiac cycles and window-based signal framing for temporal modeling (Goranthala et al., 2024).
c) Normalization, scaling, and feature standardization at the client level prior to federated updates (Akter et al., 2022).
d) Local preprocessing within client devices to prevent raw data transmission and preserve privacy.
e) Limited evaluation of how heterogeneous preprocessing pipelines affect global federated model convergence.

3.3 Model Architectures and Training Strategies

In privacy-aware healthcare federated systems, deep learning architectures typically cover CNNs, LSTMs, GRUs, hybrid CNN-LSTM designs, and multimodal sequential models. Sort of sequential models, like LSTM, are often used to grab long-term temporal connections in ECG signals (Ogbuabor, 2023) , and this general idea carries into federated settings as well. Federated xLSTM architectures, for example, extend that same ability inside decentralized environments, so they can handle multimodal ECG classification (Huan et al., 2026).

For training, most approaches use a loop of local model improvements at the client nodes, then a global aggregation step. Many papers lean on synchronized communication rounds with a fixed number of local epochs, and yes this tends to work well for classification style objectives. Yet, relatively little attention is given to continuous heart-rate forecasting when using optimized federated LSTM frameworks. Also, architectural adjustment that is specifically crafted for privacy-constrained sequential ECG modeling still feels underexplored, and not very systematically covered.

3.4 Federated Learning Algorithms Used

Federated Averaging, (FedAvg) still seems to be the main aggregation approach in healthcare federated systems (Li et al., 2021). There are a bunch of variants, they often add adaptive weighting and some client reliability tweaks, so the method stays more robust when irregular participants show up (Yazdinejad et al., 2024). On another thread, blockchain-enabled federated setups are also being proposed, partly to raise transparency and trust in decentralized medical data exchange settings (Alsamhi et al., 2024; Singh et al., 2022).

Meanwhile, edge-oriented healthcare deployments lean on communication efficient aggregation strategies to cut down bandwidth usage and the overall delay (Wang et al., 2022). But when it comes to communication-aware optimization that is tailored specifically for sequential LSTM models handling high dimensional ECG time-series data, the literature is still kind of thin , not really enough.

So overall this gap points to the need for a scalable federated optimization framework that actually matches temporal deep learning architectures.

3.5 Privacy Techniques Applied (DP, Encryption, Secure Aggregation)

In the reviewed literature, privacy-preserving mechanisms are, more or less, used like this:

α) Differential Privacy is often achieved by injecting carefully calibrated noise into gradients, or into the model parameters directly (Shi, 2025; Ghazarian et al., 2024).

β) Homomorphic Encryption is also used, so encrypted model aggregation can happen without revealing the raw updates (Aziz et al., 2023).

χ) There are secure aggregation protocols too, designed so the server can not see each individual client update, even when it wants to.

δ) In some decentralized healthcare setups, blockchain-assisted validation is used for extra transparency and auditability (Yazdinejad et al., 2023; Alsamhi et al., 2024).

ε) Hybrid frameworks combine several privacy techniques together, to dampen adversarial pressure and also reduce inference related attacks.

Despite the advancements, getting the trade off between privacy strength and computational efficiency stays a major challenge for time series applications.

4. Discussion

This part it kind of pulls together the key limitations that were spotted in earlier privacy-protecting federated learning setups for ECG, and for healthcare time-series analytics too. From what we saw in the surveyed papers, the most important research issues seem to land in three main territories: the tradeoff between privacy and model performance, the complications coming from heterogeneity plus scalability constraints, and finally the clear need for a specialized federated LSTM framework.

4.1 Privacy–Performance Trade-Off and Security Limitations

A main difficulty in federated healthcare systems is keeping strong predictive accuracy while still enforcing tight privacy guarantees. Approaches that rely on Differential Privacy add carefully adjusted noise into gradients, to shield private information (Shi, 2025; Ghazarian et al., 2024). Even though these methods are useful for dampening inference attacks, too much noise can harm convergence stability and ultimately drop classification accuracy. Likewise, Homomorphic Encryption does help confidentiality, but it also brings a notable computational delay (Aziz et al., 2023).

Federated setups combined with blockchain improve transparency and auditability (Alsamhi et al., 2024) , however they tend to create extra communication complexity. And still, federated systems are not fully safe against adversarial pressure. Examples include model poisoning, gradient leakage, and problematic or malicious client participation (Yazdinejad et al., 2023). Many current papers treat privacy and security as separate concerns, often without building a single optimization plan that can jointly preserve both robustness, and usable model performance. So reaching a favorable privacy–utility tradeoff , still remains an open research issue.

4.2 Data Heterogeneity, Communication, and Scalability Constraints

Healthcare federated environments are sort of inherently heterogeneous, because there are differences in device types, patient demographics, signal acquisition protocols, plus the institutional standards. When the ECG time-series aren't identically distributed, aka Non-IID, the global model convergence can suffer quite a lot (Li et al., 2021). A lot of the existing frameworks can simulate heterogeneity, but they do not really provide a full evaluation in conditions that feel like real multi-institutional deployments.

Then there is the communication overhead, another big constraint, especially in IoMT and edge oriented setups (Wang et al., 2022). Each round of parameter exchange during iterative training can bump up bandwidth use and add latency, which ends up limiting

scalability for real time healthcare monitoring. Also, privacy methods based on encryption add extra computational load on the client side, so the whole thing becomes less practical in resource constrained environments. For large scale rollouts across multiple hospitals, you really need communication efficient aggregation along with lighter, privacy-preserving mechanisms. But most current solutions only partially cover this issue, and that feels insufficient.

4.3 Need for a Specialized Privacy-Preserving Federated LSTM Framework

Although LSTM architectures are widely adopted for ECG time-series modeling, mostly because they can grab long-term temporal dependencies (Ogbuabor, 2023) , most federated implementations drift toward classification tasks, not continuous forecasting or heart-rate prediction. In practice, many systems rely on generic federated aggregation, and they do not really tune the optimization approach for sequential deep learning models.

So there is a rather clear need for a privacy-preserving federated LSTM framework , that is dedicated and can handle communication-efficient aggregation, calibrated privacy mechanisms, and also robustness against adversarial clients. Such a framework should, in a very explicit way, deal with ECG-specific temporal characteristics, the statistical unevenness across clients, and the limits you face during real-world deployment. Building an integrated solution that somehow balances temporal modeling efficiency with scalable, secure federated optimization is becoming an important emerging research direction in decentralized healthcare analytics.

5. Conclusion

The present review sort of systematically looked at privacy-preserving federated learning frameworks that are used for ECG and broader healthcare time-series analytics. What the literature really shows is clear progress in decentralized model training, plus the way Differential Privacy is combined with encryption mechanisms, and then how deep learning setups such as LSTM and other hybrid sequential model variations are tailored for cardiac signal analysis. Federated learning, in general, has shown it can work well for collaborative healthcare analytics while avoiding direct data sharing. At the same time blockchain tools and secure aggregation methods have helped build more trust and transparency across distributed settings. Still, a lot of the existing work mostly leans toward classification problems, and even then it is often evaluated in controlled experimental setups, not exactly in real-world, large-scale clinical deployment Even with all that, some research gaps remain pretty noticeable. One stubborn challenge is how to balance privacy protection with predictive performance, because if the privacy guarantees become stronger it often leads to accuracy degradation along with extra computational overhead, or so it seems across many papers. Another issue is data heterogeneity between institutions, especially non-IID ECG distributions, plus inconsistent preprocessing pipelines, which together can mess with global model convergence. Also, communication efficiency and scalability limitations continue to slow down practical deployment in the IoMT context and in resource-constrained healthcare systems. On top of that there are security vulnerabilities, like model poisoning and gradient leakage, and these need more robust, unified mitigation strategies rather than separate, fragmented fixes.

Future research on privacy-preserving federated ECG analysis should go toward building more optimized federated frameworks , made especially for time-series forecasting and also for real time cardiac monitoring. I mean the focus really needs to be on communication-efficient aggregation, adaptive privacy calibration, and staying robust when there are adversarial clients around, but still keeping the diagnostic reliability high. There should also be large scale validation across many institutions, standardized benchmarking datasets, and model outputs that feel clinically interpretable. That, in practice should help close the gap between these theoretical frameworks and real healthcare deployment, and so on.

REFERENCES

[1] Kusuma, S. and Jothi, K.R. (2022) 'ECG signals-based automated diagnosis of congestive heart failure using Deep CNN and LSTM architecture', *Biocybernetics and Biomedical Engineering*, 42(1), pp. 247–257.
[2] Ni, H., Meng, S., Geng, X., Li, P., Li, Z., Chen, X. *et al.* (2024) 'Time series modeling for heart rate prediction: From ARIMA to transformers', in *2024 6th International Conference on Electronic Engineering and Informatics (EEI)*. IEEE, pp. 584–589.

[3] Shiri, F.M., Perumal, T., Mustapha, N. and Mohamed, R. (2023) 'A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU', *arXiv preprint arXiv:2305.17473*.
[4] Pudikov, A. and Brovko, A. (2020) 'Comparison of LSTM and GRU recurrent neural network architectures', in *International Scientific and Practical Conference in Control Engineering and Decision Making*. Springer International Publishing, pp. 114–124.
[5] Bayer, R., Santelli, J. and Klitzman, R. (2015) 'New challenges for electronic health records: confidentiality and access to sensitive health information about parents and adolescents', *JAMA*, 313(1), pp. 29–30.
[6] Lechler, T., Wetzel, S. and Jankowski, R. (2011) 'Identifying and evaluating the threat of transitive information leakage in healthcare systems', in *2011 44th Hawaii International Conference on System Sciences*. IEEE, pp. 1–10.
[7] Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W. and Gao, Y. (2021) 'A survey on federated learning', *Knowledge-Based Systems*, 216, p. 106775.
[8] Nguyen, D.C., Pham, Q.V., Pathirana, P.N., Ding, M., Seneviratne, A., Lin, Z. *et al.* (2022) 'Federated learning for smart healthcare: A survey', *ACM Computing Surveys (CSUR)*, 55(3), pp. 1–37.
[9] Bian, M., He, G., Feng, G., Zhang, X. and Ren, Y. (2023) 'Verifiable privacy-preserving heart rate estimation based on LSTM', *IEEE Internet of Things Journal*, 11(1), pp. 1719–1731.
[10] Du, M., Wang, K., Xia, Z. and Zhang, Y. (2018) 'Differential privacy preserving of training model in wireless big data with edge computing', *IEEE Transactions on Big Data*, 6(2), pp. 283–295.
[11] Marrah, S.A., Wang, J., Koroma, A.B., Kamara, G.D., Babatunde, O.S., Marrah, M. *et al.* (2026) 'Federated deep learning for'.
[12] Huan, E., Dun, H. and Li, J. (2026) 'FedMCF-xLSTM: Federated contrastive xLSTM for multimodal multi-label ECG classification', *Biomedical Signal Processing and Control*, 116, p. 109612.
[13] Senthuran, V., Thayasivam, U., Natgunanathan, I., Sood, K. and Xiang, Y. (2025) 'Balancing privacy and health integrity: A novel framework for ECG signal analysis in immersive environments', *Computers in Biology and Medicine*, 192, p. 110234.
[14] Wani, R.U.Z. and Can, O. (2025) 'FED-EHR: A privacy-preserving federated learning framework for decentralized healthcare analytics', *Electronics*, 14(16), p. 3261.
[15] Almogadwy, B. and Alqarafi, A. (2025) 'Fused federated learning framework for secure and decentralized patient monitoring in healthcare 5.0 using IoMT', *Scientific Reports*, 15(1), p. 24263.
[16] Shi, X. (2025) 'Privacy-preserving federated learning framework for multi-institutional healthcare data analytics with differential privacy and homomorphic encryption', *Pinnacle Academic Press Proceedings Series*, 5, pp. 44–55.
[17] Wang, J., Quasim, M.T. and Yi, B. (2025) 'Privacy-preserving heterogeneous multi-modal sensor data fusion via federated learning for smart healthcare', *Information Fusion*, 120, p. 103084.
[18] Ghazarian, A., Zheng, J. and Rakovski, C. (2024) 'Privacy-preserving ECG data analysis with differential privacy: A literature review and a case study', *arXiv preprint arXiv:2406.13880*.
[19] Goranthala, V.P., Sankar, K.S. and Malar, C.B. (2024) 'Secure and privacy-preserving IoT-based arrhythmia detection with federated learning', in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, pp. 1–6.
[20] Lakhan, A., Hamouda, H., Abdulkareem, K.H., Alyahya, S. and Mohammed, M.A. (2024) 'Digital healthcare framework for patients with disabilities based on deep federated learning schemes', *Computers in Biology and Medicine*, 169, p. 107845.
[21] Alsamhi, S.H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L. *et al.* (2024) 'Federated learning meets blockchain in decentralized data sharing: Healthcare use case', *IEEE Internet of Things Journal*, 11(11), pp. 19602–19615.
[22] Yazdinejad, A., Dehghantanha, A., Srivastava, G., Karimipour, H. and Parizi, R.M. (2024) 'Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things', *Journal of Systems Architecture*, 148, p. 103088.
[23] Kumar, R., Bernard, C.M., Ullah, A., Khan, R.U., Kumar, J., Kulevome, D.K. *et al.* (2024) 'Privacy-preserving blockchain-based federated learning for brain tumor segmentation', *Computers in Biology and Medicine*, 177, p. 108646.
[24] Ogbuabor, G. (2023) *Privacy preserving context-aware framework for cardiac health monitoring*. Doctoral dissertation. Middlesex University.
[25] Yazdinejad, A., Dehghantanha, A. and Srivastava, G. (2023) 'AP2FL: Auditable privacy-preserving federated learning framework for electronics in healthcare', *IEEE Transactions on Consumer Electronics*, 70(1), pp. 2527–2535.
[26] Dasaradharami Reddy, K. and Gadekallu, T.R. (2023) 'A comprehensive survey on federated learning techniques for healthcare informatics', *Computational Intelligence and Neuroscience*, 2023(1), p. 8393990.
[27] Oh, W. and Nadkarni, G.N. (2023) 'Federated learning in health care using structured medical data', *Advances in Kidney Disease and Health*, 30(1), pp. 4–16.
[28] Aziz, R., Banerjee, S., Bouzefrane, S. and Le Vinh, T. (2023) 'Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm', *Future Internet*, 15(9), p. 310.
[29] Shen, A., Francisco, L., Sen, S. and Tewari, A. (2023) 'Exploring the relationship between privacy and utility in mobile health: Algorithm development and validation via simulations of federated learning, differential privacy, and external attacks', *Journal of Medical Internet Research*, 25, p. e43664.
[30] Sun, L. and Wu, J. (2022) 'A scalable and transferable federated learning system for classifying healthcare sensor data', *IEEE Journal of Biomedical and Health Informatics*, 27(2), pp. 866–877.
[31] Akter, M., Moustafa, N., Lynar, T. and Razzak, I. (2022) 'Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems', *IEEE Journal of Biomedical and Health Informatics*, 26(12), pp. 5805–5816.
[32] Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B. (2022) 'A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology', *Future Generation Computer Systems*, 129, pp. 380–388.
[33] Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P. and Karuppiah, M. (2022) 'Privacy-preserving federated learning for internet of medical things under edge computing', *IEEE Journal of Biomedical and Health Informatics*, 27(2), pp. 854–865.
[34] Vizitiu, A., Nita, C.I., Toev, R.M., Suditu, T., Suciu, C. and Itu, L.M. (2021) 'Framework for privacy-preserving wearable health data analysis: Proof-of-concept study for atrial fibrillation detection', *Applied Sciences*, 11(19), p. 9049.

[35] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y. *et al.* (2021) 'A survey on federated learning systems: Vision, hype and reality for data privacy and protection', *IEEE Transactions on Knowledge and Data Engineering*, 35(4), pp. 3347–3366.
[36] Kaur, Shabad and Virk, Amandeep Kaur (2015) 'AODV Extension Using Genetic Algorithm in VANET', *International Journal of Science and Research (IJSR)*, 4(7), July. ISSN 2319-7064.