Scientific Reports

https://doi.org/10.1038/s41598-026-40964-y

Article in Press

Federated learning with continual update for privacy-preserving clinical event prediction across distributed hospitals using MCN-GNN

Received: 21 November 2025

Accepted: 17 February 2026

Published online: 08 March 2026

Cite this article as: Jagdeesh K., Kanimozhi N., Sardar T.H. *et al.* Federated learning with continual update for privacy-preserving clinical event prediction across distributed hospitals using MCN-GNN. *Sci Rep* (2026). https://doi.org/10.1038/s41598-026-40964-y

K. Jagdeesh, N. Kanimozhi, Tanvir H. Sardar, N. Naveenkumar, B. Mahalakshmi, A. Chandrasekar, M. Karpagam & Sk Mahmudul Hasan

FEDERATED LEARNING WITH CONTINUAL UPDATE FOR PRIVACY-PRESERVING CLINICAL EVENT PREDICTION ACROSS DISTRIBUTED HOSPITALS USING MCN-GNN

K. Jagdeesh [1], N Kanimozhi [2], Tanvir H Sardar [3], N. Naveenkumar [4], B.Mahalakshmi [5], A. Chandrasekar [6], Karpagam M [7*], Sk Mahmudul Hasan [8*]

[1] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai 600062, Tamil Nadu, India.*

[2] *Department of Computational Intelligence, Faculty of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Chennai, Tamil Nadu 603203, India.*

3 Dept of CSE, School of Engineering, Dayananda Sagar University, Bengaluru 562112, India

[4] *Department of Information Technology, Nehru Institute of Technology, Kaliyapuram, Coimbatore-641 105, Tamil Nadu, India.*

[5] *Department of Computer Science and Engineering, M.P.Nachimuthu M.Jaganathan Engineering College, Erode, Tamil Nadu, India,*

[6] *Professor and Head, Department of Computer Science and Engineering, Nandha College of Technology, Erode-638052, Tamilnadu, India.*

[7] *Department of Computational Intelligence, Faculty of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Chennai 603203, Tamil Nadu, India.*

[8] *Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India, 560064*

Contributing author : drjagadeeshk@veltech.edu.in, kanimozn@srmist.edu.in, tanvir.sardar@gmail.com, nnaveenkumar.dr@gmail.com , maharajan2203@gmail.com, chandru.as1312@gmail.com

Corresponding author *: karpagam1@srmist.edu.in, mahmudul.hassan@manipal.edu

Abstract: Federated Learning (FL) enables accurate and secure Clinical Event Prediction (CEP) across distributed hospitals. However, the prevailing works overlooked the catastrophic forgetting during the global update. Therefore, a Meta Experience Polynomial Decay-based Replay (MEPDR)-centric continual update is proposed. Initially, the hospitals (local model) register and log into the blockchain. Then, to train the CEP model, data collection, pre-processing, and feature extraction are performed. Further, the Temporal-Causal Graph (TCG) is constructed. Afterward, the node matrix is created, and the CEP is done using Mean-Centering Normalization-based Graph Neural Network (MCN-GNN). The model's gradients are further preserved using the Homomorphic Robust Log Scaling-based Encryption (HRLSE). Next, the hospitals are authenticated using the Exponential Probing Digital Signature Algorithm (ExPrDSA). Thereafter, in the global model, the aggregation is performed using the Calinski–Harabasz Index with Zhonghua Distance-based K-Means Clustering (CHIZD-KMC), followed by global CEP. After that, during the global update, the MEPDR-based continual learning is carried out in each local model. Also, the transactions are stored in the blockchain

to enhance traceability. Thus, the proposed system effectively predicted the clinical events with an accuracy of 98.97%, outperforming existing works.

Keywords: *Federated Learning, Graph Neural Network (GNN), Clinical Event Prediction, Distributed Healthcare Systems, Medical Informatics, Electronic Health Records, Secure Clinical Artificial Intelligence, and Deep Learning (DL).*

1. INTRODUCTION

The development of Artificial Intelligence (AI), especially in the healthcare system, has transformed a wide range of domains. The healthcare with predictive models helps in the diagnosis and treatment planning [1, 2]. In CEP, the Electronic Health Record (EHR) of the patient is analyzed and correlated to improve patient outcomes [3]. However, these healthcare data are often fragmented, thus causing restrictions on centralized data sharing [4]. Therefore, FL has been developed to enable multiple hospitals for collaboratively training the global models without transferring the data of patients [5]. This enables privacy preservation in the distributed healthcare system.

During the deployment of federated learning in real-world environments, the format of the electronic health records and the heterogeneity of the data must be considered [6]. The existing works converted the EHR into an effective format for clinical event prediction. The DL models, like Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM), were widely used in the prevailing works for clinical event prediction [7, 8]. However, the higher-order dependencies couldn't be captured by these models [9]. Thus, the GNN that represented the clinical events as nodes and relationships as edges was utilized to analyse the patterns in EHR [10]. Some prevailing works integrated GNN with federated learning to provide scalable and privacy-preserving CEP across distributed hospitals.

Nevertheless, the traditional FL-based clinical event prediction models exhibited significant limitations [11]. The prevailing models shared the gradients without privacy preservation into the global model. This resulted in inference of attacks and improper CEP [12]. Also, the global model's performance was degraded due to the participation of malicious hospitals in the distributed hospital network [13]. In the prevailing works, the coordination between diverse participants became complex due to the absence of transparent records [14]. Furthermore, adapting to the shared knowledge without losing the local credits remained a challenge [15]. The motive of the paper is to safeguard the sensitive patient information and resist the adversarial interference with precise FL-based CEP. Hence, a novel MEPDR-based continual update and MCN-GNN-based CEP is proposed.

1.1 Problem Statement

The drawbacks present in the prevailing works are described as follows,

- None of the prevailing works overcame the catastrophic forgetting, thus resulting in a drop in performance in predicting the clinical events after the global update.
- In the existing [16], sharing model gradients without encryption caused attackers to exploit the patterns through model inversion attacks, leading to serious privacy risks.
- In the prevailing [17], FL was vulnerable to malicious hospitals that send adversarial model updates, thus degrading the global model's performance and reliability.
- Many hospitals distrusted centralized aggregation servers due to a lack of transparent and verifiable records of participation [18].

- In prevailing [19], directly aggregating updates from heterogeneous local models led to misalignment and unreliable global model updates.

- Most of the existing models learned patterns based on connections and correlations in data rather than true causal relationships. Thus, the performance of the prediction was reduced.

Core Contribution of the Proposed Work: Here, the proposed work develops a federated learning with continual update for privacy-preserving clinical event prediction across distributed hospitals. Also, the proposed work addresses catastrophic forgetting in distributed hospital settings through MEPDR, ensuring continual learning without loss of local expertise. Further, the prediction accuracy is enhanced by constructing the Temporal causal graphs and using the MCN-GNN while mitigating over-smoothing. Moreover, the privacy during model gradient updation is preserved using the HRLSE, whereas the hospital authentication is strengthened using the ExPrDSA. Further, to improve aggregation reliability, the CHIZD-KM is applied for cluster-wise updates. Finally, blockchain integration confirms transparent, immutable traceability of all transactions, making the system secure across distributed hospitals.

1.2 Objectives

The contributions of the proposed approach are given below,

- ✓ The MEPDR-based continual update is provided to the local model during the global update. This helps in overcoming the catastrophic forgetting issue and increases the prediction performance.
- ✓ For the privacy preservation of the local model's output gradients, the HRLSE method is utilized. Thus, the model inversion attack is avoided.
- ✓ To avoid adversarial model updates and to enhance the global model's performance, the hospitals are authenticated using ExPrDSA.
- ✓ The transparent and verifiable record of participation with fairness and accountability is provided by storing all the transactions in the blockchain.
- ✓ To aggregate the heterogeneous data from the local models into the global model, the cluster-wise aggregation is performed using the CHIZD-KMC approach.
- ✓ For learning the causal relationship and the correlation of the electronic health records data, the TCG is constructed and further utilized for MCN-GNN-based clinical event prediction.

The paper is structured as: The related works are explained in Section 2, the proposed method is described in Section 3, the performance of the proposed system is analyzed in Section 4, and lastly, the paper is winded up in Section 5 with future scope.

2. LITERATURE SURVEY

[16] presented FL for privacy-preserving of the EHR in clinical research. The EHR for multiple institutions was collected. Then, the classifier models, such as Logistic Regression, Support-Vectors-Classifiers, Decision-Tree-Classifiers, Random-Forests, and Stacking-Classifiers, were utilized for disease diagnosis. Here, the FL was used to enhance privacy preservation. Thus, the disease was effectively detected. However, the sensitive information was not preserved, thus leading to serious privacy risks during data sharing. Also, [17] established private client selection and resource allocation in FL for medical applications. Here, the

medical information of the patients was collected from the distributed hospitals. Then, the GNN was utilized for the detection of clinical events. Next, the aggregation of the data into the local model was carried out by client selection. Hence, the CEP with privacy was maintained. Nevertheless, the hospitals were not authenticated. Thus, the malicious hospitals sent adversarial model updates, degrading the model's performance. Furthermore, [18] developed an FL model with dynamic scoring-centric client selection for disease diagnosis. At first, the server was initialized, and the local training was carried out using a random forest. Then, the output of the model was aggregated based on the dynamic score. Further, the global model was trained centered on the aggregated data in the FL. Thus, the disease was precisely diagnosed. On the other hand, the model lacked transparent and verifiable records of participation, thereby reducing the reliability of disease prediction. Similarly, [19] estimated a graph-centric model for anomaly detection in healthcare using FL. Here, the EHR data was collected from the patients. Then, the data was integrated using Kafka, and the real-time processing was carried out. Further, the local model was trained using the Convolutional Neural Network and LSTM (CNN-LSTM). Then, the gradients were aggregated, and the global model was updated. Afterward, based on multimodal attention, the anomaly score was predicted; then, the alert was generated effectively. But, the direct aggregation led to misalignment of global model updates. Additionally, [20] introduced a privacy-preserving FL framework for scalable and secure healthcare investigation. Here, the healthcare data was collected from the data owner and stored in each hospital. Next, the Homomorphic Encryption (HE) was applied to each local model's data. Then, the security was validated in the homomorphic computation unit, and the regulatory compliance was also applied. Next, the large-scale data was transferred into the global model for further processing. Hence, the privacy of the healthcare data was effectively preserved. Yet, the gradient stability of the model was improper, thus degrading the local update.

Moreover, [21] explored the security of EHR using the trusted decentralized FL consensus mechanism. The doctor and patient logged into the blockchain. After that, the EHRs of the patients were collected, and the missing values were imputed. Subsequently, the data were normalized utilizing the min-max technique. Thereafter, the features were selected. By utilizing a Generative Adversarial Network (GAN), the disease was predicted. These gradients were further transferred to the cloud server that had a local model. Thus, the prediction of the disease was precisely carried out. However, due to catastrophic forgetting, the local model couldn't predict the disease, leading to a performance drop. Also, [22] demonstrated a multi-source EHR prognosis identification via a privacy-preserved FL approach. Here, a privacy-aware multi-channel architecture securely embedded every single clinical feature separately in clinical representation learning. This framework allowed every individual to maintain their sensitive clinical information, showing high reliability. But, this model had considerable latency in model updates aggregation, thereby resulting in outdated global models. Further, [23] utilized an advanced framework named FL-based privacy preservation in healthcare systems. Here, a privacy-preserving methodology like a secure multi-differential privacy model was employed to ensure data privacy. Then, the secured data was analyzed, and the gradients were transferred to the server. Thus, the privacy was preserved, and the diagnosis was carried out. However, the cause-and-effect relationship was not analysed, thus reducing the diagnosis performance. Next, [24] employed a serverless privacy edge intelligence-centric federated learning model in smart healthcare systems. In this work, the federated edge aggregator and authentication methodology were included to enhance data privacy and enable client adaptation. Here, the model classified the intruders via serverless computing processes. Hence, it attained higher accuracy and provided enhanced medical security with serverless computing. Nevertheless, the model increased the processing delay. Likewise, [25] introduced a framework for false-positive-tolerant misconduct mitigation in distributed federated learning in clinical institutions.

Here, the false-positive tolerant methodology was established for preserving model integrity and mitigating the effects of adversarial misconduct in FL. The model prevented over-ostracization and the subsequent loss of sample size. However, the model still had issues with heterogeneous data quality and varying record-keeping standards across clinical institutions.

Additionally, [26] implemented a medical diagnosis model using Graph Neural Networks (GNN) for medical images. At first, the medical images were segmented into regions of interest and further normalized. Next, they were represented as a graph and fed into a structural GNN. Finally, a multi-task learning approach was employed within the GNN to handle disease classification and severity prediction. As a result, the model attained 92.27% Area Under the Curve (AUC). Nevertheless, the model suffered from noise sensitivity and over-smoothing limitations, causing reduced learning efficiency. Similarly, [27] presented a Federated-Decentralized-Learning Graph Attention Network for Doctor Recommendation (FD-GATDR) model using Electronic Health Records (EHRs). The model utilized Bi-directional Encoder Representations from Transformers-Long Short-Term Memory (BERT-LSTM) for service code embedding. Then, the Heterogeneous Graph Attention Network (HGAT) was utilized to learn structured representations from EHR data. Further, Federated Decentralized Learning (FDL) handled decentralized data. Hence, the model improved AUC by up to 6.2%. However, the model had low communication efficiency when handling complex heterogeneous graph structures. Also, [28] developed a patient-centric preictal pattern-aware epileptic seizure detection based on federated learning. The spiking encoder with a graph convolutional neural network served as the local model, which was trained using a bi-timescale approach. Centered on the federated learning outcomes, the adaptive neuro-fuzzy inference system was used to identify the epileptic seizure patients. Here, the three-tier architecture for epileptic seizure prediction was presented to improve the model's learning capability while maintaining data privacy. This model offered fine-grained personalization. However, this framework struggled to handle the high dynamics of epileptic EEG signals, causing classification errors. Finally, [29] propounded an integrated federated learning with a split learning framework for brain disease prediction using a spatio-temporal graph network. Here, federated learning and spatial learning techniques were applied. A time-aware scheme was applied in the client temporal model to capture the functional changes in the brain structure. In the server spatial model, a graph convolutional neural network was integrated with federated learning. This model significantly improved the diagnostic efficiency through a federated learning scheme. But, this scheme had considerable latency owing to the complex architecture.

Overall, the existing federated learning and GNN-based healthcare models suffer from key limitations, such as weak gradient privacy, lack of authentication, over-smoothing in graph learning, catastrophic forgetting in continual updates, high communication latency, and absence of verifiable audit trails. Therefore, by integrating the MCN-GNN, HRLSE, ExPrDSA, and MEPDR with the proposed work, the proposed work effectively addresses the above mentioned limitations and provides high accuracy during clinical event prediction. Also, the proposed work ensures security, stability, and scalability in federated clinical event prediction compared to traditional works.

3. PROPOSED METHODOLOGY FOR PRIVACY-PRESERVING CLINICAL EVENT PREDICTION VIA FEDERATED LEARNING

In the proposed work, privacy is preserved, and the FL-based clinical event prediction is carried out regarding the EHR. The important steps involved in the proposed framework are TCG construction, CEP, model gradient privacy-preservation, hospital authentication, cluster-wise

aggregation, and continual update in the local model. The structure of the proposed system is demonstrated in Figure 1.

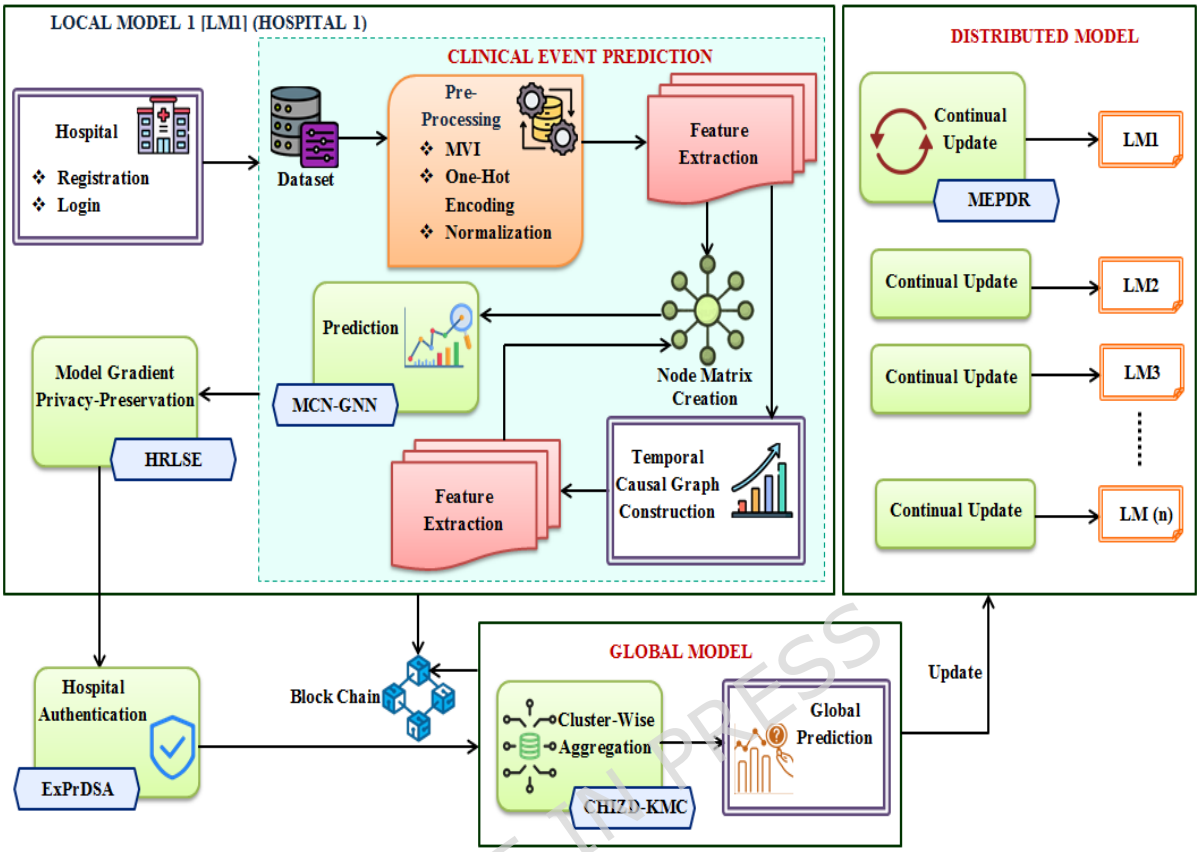


Figure 1: Architecture of the Proposed Framework

In the proposed work, the proposed MCN-GNN is introduced for excellently performing CEP. Also, the proposed HRLSE is employed to secure the output gradient of the local model. For avoiding the adversarial model updates, the hospital authentication is performed using the proposed ExPrDSA. Likewise, the proposed CHIZD-KMC is employed to aggregate the heterogeneous data from the local models into the global model. To avoid the catastrophic forgetting issue, increase the prediction performance, and eliminate the overfitting issue, the proposed MEPDR is used for continual update during global update.

In the proposed FL system, there are a (n) number of local models, which act as distributed hospitals (H). All these (H) are heterogeneous, i.e., some models predict stroke, some diagnose heart failure, and so on. Here, the (n) number of local models is trained for CEP regarding heart failure EHR, stroke data, and cirrhosis prediction data. Eventually, all the trained local models are updated in the global model.

3.1 Local Model 1

In this proposed approach, the local model 1 is trained for clinical event prediction based on the heart failure EHR. The processes carried out in the local model 1 are explained in the following sections.

3.1.1 Hospital Registration and Login

At first, the registration of Local Model 1 (Hospital 1) (H_1) into the blockchain is carried out. Here, due to the nature of the blockchain, such as decentralisation, immutability, and transparency, each hospital's identity and registration details are securely recorded, preventing unauthorised access and tampering. However, without blockchain, the registration process relies on a centralised server, which is vulnerable to single-point failures, unauthorised access, and data tampering. Also, the blockchain layer functions as a thin trust mechanism, making the architecture both secure and feasible for real-world multi-hospital deployments. Therefore, the hospital registration is carried out on the blockchain network. In this, the registration and login of (H_1) are done based on the hospital Identification (ID) and password. Further, the CEP is performed.

3.1.2 Clinical Event Prediction

Here, to predict heart failure, the clinical event prediction model is trained. For training, the data collection, pre-processing, feature extraction, TCG construction, and prediction are done. The step-by-step process for training the CEP model is described as follows,

3.1.2.1 Dataset

The heart failure prediction dataset, which consists of EHR, has been collected. The data (E) from this dataset is utilized for the training of (H_1). Here, the total (h) number of data is available. Next, (E) is pre-processed.

3.1.2.2 Pre-Processing

Thereafter, to convert (E) into a structured format and to ensure reliable analysis of the data, the pre-processing steps, namely Missing Value Imputation (MVI), one-hot encoding, and normalization, are done.

- ***Missing Value Imputation***

Primarily, the missing values in (E) are filled using the MVI process. Here, the mean of the neighbouring value in the dataset is used for imputing the missing data. By filling in the missing values, the data is made compatible. Let the MVI output be represented as (E'').

- ***On-Hot Encoding***

Afterward, the categorical variables present in (E'') are converted into a binary vector using One-Hot Encoding (OHE). This process identifies the categorical variables in (E'') and assigns a binary vector for each category. Thus, the DL models efficiently process the data. The output of OHE is signified as $(\dddot{E})$.

- ***Normalization***

Then, $(\dddot{E})$ is normalized in the range of 0 to 1 using the min-max normalization technique, which is provided in equation (1). This helps in preserving the original data distribution and trains the CEP model precisely.

$$\tilde{E} = \frac{\ddot{\ddot{E}} - \ddot{\ddot{E}}^{min}}{\ddot{\ddot{E}}^{max} - \ddot{\ddot{E}}^{min}} \tag{1}$$

Here, $(\tilde{E})$is the normalized output, $(\ddot{\ddot{E}}^{\min}, \ddot{\ddot{E}}^{\max})$are the minimum and maximum values of $(\ddot{\ddot{E}})$, respectively, and $(\tilde{E})$is the final pre-processed data. After that, features are extracted from $(\tilde{E})$ for further analysis.

3.1.2.3 Feature Extraction

Next, from$(\tilde{E})$, the features, namely age, resting blood pressure, sex, chest pain type, cholesterol level, resting electrocardiogram results, maximum heart rate achieved, old peak, fasting blood sugar, exercise-induced angina, and so on, are extracted. The extracted features are denoted as (F). Further, the TCG is constructed.

3.1.2.4 Temporal-Causal Graph Construction and Feature Extraction

In this section, to capture the cause-and-effect relationships between clinical events over time in(F), the TCG is constructed. TCG excellently provides differentiation of true cause and effect relationships from mere correlations. The TCG analyzes whether earlier event data influences the later one or not. The features(F)act as nodes (events)(y), and the links with temporal constraints(g)serve as edges(z). Next, for capturing the temporal influences, lagged vectors are generated to a maximum lag (ℓg). Afterward, the temporal causal relationship is analyzed for identifying how the variable relies on its past values and its causal parent values change at earlier times.

$$\varepsilon\varpi_{ab\to mn} = \frac{1}{nT-1}\sum_{tm=\ell g+1}^{nT} y_{ab}(tm-\ell g)y_{mn}(tm) \tag{2}$$

Where, $\varepsilon\varpi_{ab\to mn}$ specifies the edge weight, nT indicates the number of time steps (tm), and y_{ab} and y_{mn} signify the ab^{th} and mn^{th} nodes, correspondingly. Then, the $\varepsilon\varpi_{ab\to mn}$ are normalized to prevent the relative causal influence, and it is represented as $\overline{\varepsilon\varpi}_{ab\to mn}$. Thereafter, edge thresholding is carried out. Next, the temporal causal adjacency matrix (αd_{mnab}) is defined as,

$$\alpha d_{mnab} = \begin{cases} \text{if} \quad er_{ab\to mn} \in z & \overline{\varepsilon\varpi}_{ab\to mn} \\ \text{otherwise} & 0 \end{cases} \tag{3}$$

Here, $er_{ab\to mn}$ denotes the directed edges. Also, node-level connectivity strength is analyzed. Thus, the constructed TCG$(\Im)$is given in equation (4) as,

$$\Im = [F, y, z, \varepsilon\varpi_{ab\to mn}] \tag{4}$$

Then, from $(\Im)$, features are extracted. The TCG-based features(N), like in-degree, out-degree, weighted degree, edge weights, statistical confidence of causal links, strongly connected components, causal chain lengths, temporal motifs, node, and so on, are extracted

from $(\Im)$. Here, the total (l) number of TCG-based features exists. Further, the node matrix is created.

3.1.2.5 Node Matrix Creation

Subsequently, the node matrix (K) is created based on the features (F, N) from pre-processed data and TCG, respectively. This (K) is given as input to the proposed CEP classifier.

$$K = (F, N) H_1 \tag{5}$$

Afterward, (K) is fed into the MCN-GNN classifier.

3.1.2.6 Prediction

In this phase, the clinical event is predicted based on the created node matrix (K) using MCN-GNN. The GNN that captures complex relationships between nodes (clinical events) and edges (features) for large-scale information is used for heart failure CEP. It also captures the higher-order dependencies across the entire EHR of a patient. Also, it has excellent parameter sharing and strong inductive capabilities. Normally, a GNN consists of two layers, such as message passing and node update. Yet, the GNN has an over-smoothing issue, i.e., all nodes tend to become indistinguishable from each other after several layers of message passing, thus reducing the discrimination and classification performance. Therefore, various smoothing approaches like Min-Max Scaling, Z-Score Normalization, and Mean-Centering Normalization (MCN) are supported for node stabilization from over-smoothing. Among them, MCN is considered as the best function since Min-Max Scaling and Z-Score Normalization handle either mean shift or scale, leading to ineffective preservation of node-level distinctions across layers. MCN diminishes the excessive feature averaging and improves the robustness by preserving node-specific information, ensuring that each clinical event retains its unique representation. Also, MCN enhance the GNN's ability to capture higher-order dependencies across the entire HER without losing discriminative power, thus improving the classification accuracy of heart failure prediction. The architecture of the MCN-GNN classifier is depicted in Figure 2.

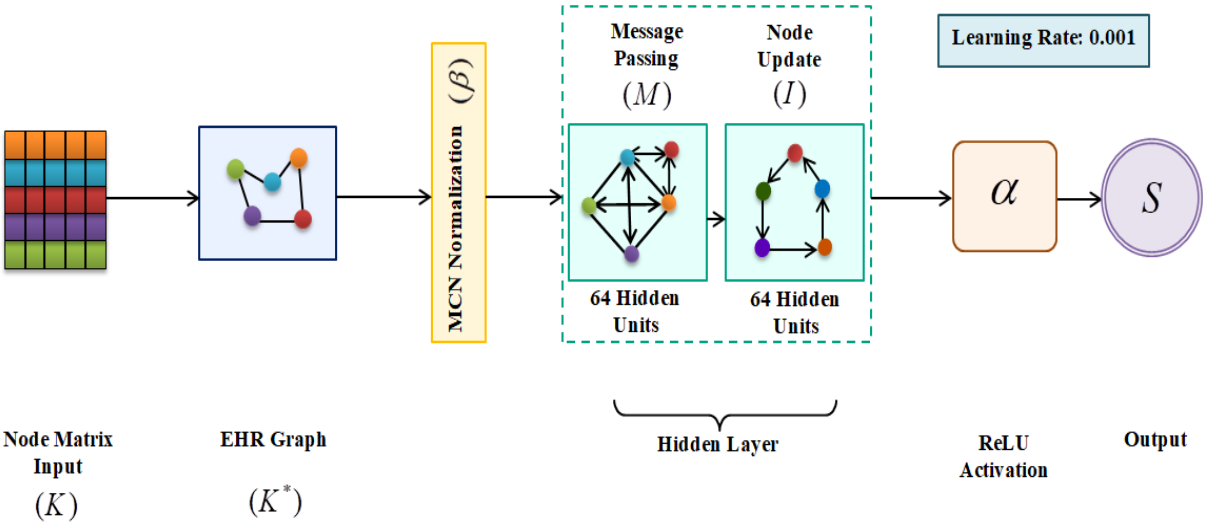


Figure 2: MCN-GNN Classifier

➲ ***EHR Graph***

The node matrix (K) is fed into the MCN-GNN model. Primarily, (K) is utilized to generate the EHR graph (K^*). Here, (K^*) is constructed to model the relationship of the features (nodes) across time (t). Also, (K^*) helps the model to learn correlations and interaction patterns within patient health information.

$$K^* = [K] \times t \tag{6}$$

Then, the reduction of node complexity is performed to keep the most informative clinical features.

➲ ***Normalization***

Then, to prevent over-smoothing and to differentiate the nodes with less complexity, the MCN is applied to (K^*). The MCN reduces the drift across layers and preserves all the individual node features. The MCN output (β) is expressed in equation (7) as,

$$\beta = \left\langle \frac{K_1^* + K_2^*}{2} \right\rangle * K^* \tag{7}$$

Here, (K_1^*, K_2^*) are the two nodes of (K^*). Next, the processing of (β) is carried out in the hidden layer of the proposed classifier.

➲ ***Hidden Layer***

In the hidden layer, the message passing and the node update are carried out. This helps in capturing the higher-order dependencies in EHR data. Also, the hidden layer effectively learns complex clinical relationships.

Message Passing

Initially, the message passing (M), which is said to be neighbourhood aggregation, is performed. Each node in (β) collects information from its connected neighbours and analyzes the cause-and-effect and correlation between the input data.

$$M = \{[M * \chi] + \delta\} \times \alpha \tag{8}$$

$$\alpha = \max(0, \beta) \tag{9}$$

Where, (χ, δ) are the weight and bias values of (β), correspondingly, and (α) is the Rectified Linear Unit (ReLU) activation function that introduces non-linearity and learns complicated patterns and relationships within the input data.

Node Update

After that, the aggregated data (M) is combined with the node's current state to produce a new state that encodes global contextual knowledge and local feature information.

$$I = \beta + M \tag{10}$$

Here, the node update output is represented as (I), which is provided in equation (10).

➲ ***ReLU Activation***

Further, the ReLU activation is done in the readout layer. Here, the summation of the nodes and activation is done to represent the data in a single vector (U). ReLU improves non-linear separability and suppresses inappropriate negative activations.

$$U = \left\{\left[\sum I * \chi\right] + \delta\right\} * \alpha \tag{11}$$

Thus, the final heart failure CEP output (S) is predicted in the feed-forward layer. The prediction output of the local model 1 (Hospital 1) is depicted as,

$$S = \alpha \times \left\langle\left[U * \chi\right] + \delta\right\rangle \tag{12}$$

$$S = \left\langle S_1, S_2 \right\rangle \tag{13}$$

Where, (S_1, S_2) are the normal and heart disease classes, respectively. Hence, the clinical event prediction of the local model 1 is carried out. The pseudocode for MCN-GNN is given as follows,

Pseudo-code for MCN-GNN

Input: Node Matrix (K)

Output: Heart Failure CEP output (S)

Begin

Initialize (χ, δ)

For (K)

Construct EHR graph

$K^* = [K] \times t$

Apply normalization to prevent over-smoothing

$$\beta = \left\langle \frac{K_1^* + K_2^*}{2} \right\rangle * K^*$$

//**Hidden** layer

Estimate ReLU activation

$\alpha = \max(0, \beta)$

While (β)

Message passing $M = \left\{\left[M * \chi\right] + \delta\right\} \times \alpha$

Update node $I = \beta + M$

ReLU activation in readout layer

$$U = \left\{\left[\sum I * \chi\right] + \delta\right\} * \alpha$$

Detect heart failure $S = \alpha \times \left\langle\left[U * \chi\right] + \delta\right\rangle$

End while

End for

Return Heart Failure CEP output $S = \langle S_1, S_2 \rangle$

End

In real time, when the EHR data is entered by Hospital 1 (H_1), the heart failure of the patient is predicted. Next, the gradients (R) of (S) are preserved.

3.1.3 Model Gradient Privacy Preservation

Afterward, to secure the output gradient of the local model 1, the HRLSE is used. The traditional lightweight encryption techniques like Elliptic Curve Cryptography (ECC), HE, Rivest-Shamir-Adleman (RSA), and Advanced Encryption Standard (AES) are well-suited for enhancing data security and privacy preservation. Amongst them, the HE is a powerful cryptographic model that significantly reduces the risk of data leakage while preserving sensitive information. Also, it enables computations to be performed directly on encrypted data without the need for decryption. The HE helps to prevent model inversion attacks by encrypting the model's gradient (R), thus ensuring that the data is never exposed. The attackers can't directly inspect the data mapping, making it impossible to infer the model's gradient. On the contrary, noise is known as a random error that is added to ciphertexts during encryption, thereby making the distributions indistinguishable. Therefore, various scaling models like Log Scaling, Box-Cox Transform, and Robust Log Scaling (RLS) help to control the noise growth. Among these, the RLS is selected as the log scaling and box-cox transform approaches are sensitive to outliers. RLS avoids the noise growth produced by continual homomorphic additions and multiplications. Also, by integrating RLS with HE, the proposed HRLSE achieves efficient and accurate gradient encryption while preventing excessive noise accumulation during repeated homomorphic operations.

Initially, to avoid the accumulation of noise during privacy preservation, the RLS that limits the amplification of noise and maintains features distinctness is applied to (R). By scaling (R), the large gradient magnitudes are compressed into a controlled range, thereby mitigating the noise or outlier accumulation. The RLS output $(\ddot{R})$ is expressed in equation (14) as,

$$\ddot{R} = R * \log\left[\frac{|R|}{q} + 1\right] \tag{14}$$

Where, log implies the logarithmic function and (q) is the constant for numerical stability. Next, the public key (ε) and private key (ϕ) utilized for the encryption of the input data $(\ddot{R})$ are generated.

$$\varepsilon = \ddot{R} + (d, e) \tag{15}$$

$$\phi = \varepsilon + \ddot{R} \tag{16}$$

Here, (d, e) are the noise parameters. Finally, to avoid the model inversion attack and loss of gradient information, the encryption is performed regarding (ε) and (ϕ). The privacy-preserved gradient of the local model 1 (G) is given in equation (17) as,

$$G = \vec{R}(d, e) + \varepsilon + \phi \tag{17}$$

Hence, in the FL system, the model's output is secured throughout the prediction process. Thereafter, Hospital 1 is authenticated. Similarly, the Local model 2 is trained based on the stroke prediction dataset for identifying whether the patient has a stroke or not. Also, the Local model 3 is trained regarding the cirrhosis prediction dataset for detecting cirrhosis disease (liver disease). Likewise, all the (n) number of local models are trained and finally updated in the global model.

3.2 Hospital Authentication

Next, (G) is transferred to the global model of the FL system. Before transferring (G), Hospital $1(H_1)$ is authenticated using ExPrDSA. The Digital Signature Algorithm (DSA) is relatively faster in generating a large number of digital signatures, thus rapidly performing the authentication. Also, DSA ensures that the information has not been tampered with during transmission. However, the hash function used by the DSA for generating signatures can be hacked, resulting in information loss and improper authentication. Thus, in DSA, the hash function is generated with the help of linear activations, sigmoid activations, or the Exponential Probing (ExPr) function. Here, the linear and sigmoid actions are vulnerable to collision or hash-flooding attacks, affecting the authentication robustness. Therefore, the ExPr is applied to generate a hash function, which makes collision prediction harder and improves the robustness against hash-flooding attacks; also, it avoids information loss. Additionally, by incorporating the ExPr function with the DSA, the proposed ExPrDSA becomes more resilient to cryptographic attacks, thereby ensuring that digital signatures remain secure even under adversarial conditions.

Primarily, the digital signature is created based on the Hospital ID (T), public key (ε), and the hash function (γ). As explained in Section 3.1.3, the public key (ε) is generated. Moreover, to avoid hacking, a hash function (γ) is generated using the ExPr function, which makes the hash less predictable and harder to exploit. Likewise, the ExPr function allows enhanced resistance to adversarial collisions.

$$\gamma(H_1) = (u) + \exp\{\mathrm{mod}[T(H_1)]\} \tag{18}$$

Here, (u) is the constant value, $(\exp)$ is the exponential function, and (mod) is the modulus operator. Based on (γ), (T), and (ε), the digital signature $D(H_1)$ is created for hospital 1.

$$D(H_1) = T(H_1) + \gamma(H_1) + \varepsilon \tag{19}$$

This $D(H_1)$ is given to the global model for authentication. After that, the global model (Q) generates $\gamma(Q)$ using $G(H_1)$.

$$\gamma(Q) = (u) + \exp\{\mathrm{mod}[T(H_1)]\} \tag{20}$$

Further, the digital signature $D(Q)$ at the global model is generated using (T), (ε), and $\gamma(Q)$.

$$D(Q) = T(H_1) + \gamma(Q) + \varepsilon \tag{21}$$

Thereafter, the digital signature verification is done regarding $D(H_1)$ and $D(Q)$ for the authentication of hospital 1 (H_1) and to transmit the privacy-preserved gradient (G) into (Q). The hospital authentication output (J) is given in equation (22) as,

$$J = \begin{cases} if\ D(H_1) = D(Q) & J^1 \\ if\ D(H_1) \neq D(Q) & J^2 \end{cases} \tag{22}$$

Where, (J^1, J^2) are the hospital authenticated and non-authenticated outputs, respectively. The condition states that if the generated digital signatures on the hospital and global model sides are equal, then (H_1) is said to be authenticated (J^1). If the digital signatures are not equal, then (H_1) is said to be non-authenticated (J^2). The pseudo-code for ExPrDSA is given as follows,

Pseudo-code for ExPrDSA

Input: Hospital ID (T), Public Key (ε)

Output: Hospital Authentication Output (J)

Begin

Initialize (u)

For (H_1)

Estimate hash value

$$\gamma(H_1) = (u) + \exp\{\mathrm{mod}[T(H_1)]\}$$

Determine digital signature

$$D(H_1) = T(H_1) + \gamma(H_1) + \varepsilon$$

End for

For (Q)

Identify hash value

$$\gamma(Q) = (u) + \exp\{\mathrm{mod}[T(H_1)]\}$$

Generate digital signature

$$D(Q) = T(H_1) + \gamma(Q) + \varepsilon$$

End for

While $D(H_1), D(Q)$

//**Hospital** authentication

If $D(H_1) = D(Q)$

Hospital 1 authenticated (J^1)

Else if $D(H_1) \neq D(Q)$

Hospital 1 non-authenticated (J^2)

End if

End while

Attain Hospital Authentication Output (J)

End

Thus, if (J^1) is attained, then the privacy-preserved gradient (G) is transmitted to (Q); if (J^2) is attained, then the transmission of (G) is blocked. Hence, the authentication of hospital 1 is carried out effectively. Further, the aggregation of gradients from all the local models is done.

3.3 Global Model

In this phase, the gradients from the authenticated heterogeneous hospitals $J^1(H)$ are collected and aggregated. Then, the global prediction, which is the main part of the FL, is done.

3.3.1 Cluster-wise Aggregation

Initially, the cluster-wise aggregation of the gradient (G) related to different disease diagnosis outputs from $J^1(H)$ is performed using the CHIZD-KMC approach. Here, the K-Means Clustering (KMC) that automatically partitions the participating hospitals into clusters based on the similarity of their local model gradient (G) is used for aggregation. This enables cluster-wise aggregation in the global model and ensures that updates from hospitals with similar data distributions are aggregated together to improve convergence. However, KMC is sensitive to the initial placement of centroids, leading to inconsistent results. Moreover, diverse initializations can cause the KMC to converge to different local minima. Additionally, the reliance on Euclidean distance misrepresents the data and fails to capture the true structure of the data, causing suboptimal clustering and poor cluster formation. Among the various centroid initialization techniques, like Silhouette index, Dunn index, and Calinski–Harabasz Index (CHI), the CHI is effective because the silhouette and Dunn indexes are sensitive to the cluster shapes, affecting the overall performance. Therefore, the CHI, which encourages initial centroid placement by maximizing the ratio of between-cluster dispersion to within-cluster dispersion, is used. Also, in KMC, the Zhonghua Distance (ZD) is used instead of Euclidean distance, Manhattan distance, or Cosine Similarity. Here, the Euclidean, Manhattan, or cosine demonstrate poor performance in non-linear and high-dimensional spaces. Hence, the Zhonghua Distance (ZD) is applied to compute the distance by integrating distribution-aware deviations between data points and centroids; also, ZD diminishes the sensitivity to noise and outliers. Further, the proposed CHIZD-KMC achieves more consistent and robust clustering of participating hospitals, ensuring that hospitals with similar local model gradients are grouped accurately using the CHI-based centroid initialisation and ZD-based distance measurement.

Let the gradients (G) attained from $J^1(H)$ be represented in equation (23) as,

$$G = \left\{G\left[J^1(H_1), J^1(H_2), J^1(H_3), J^1(H_4), ..., J^1(H_n)\right]\right\} \tag{23}$$

Here, (n) is the number of distributed hospitals. Next, the centroid (L) from the total gradients (G) attained is selected using the CHI, which provides a clear numerical measure of cluster quality and diminishes unnecessary iterations.

$$L = \frac{\eta^1}{\eta^2} * \left[\frac{n(G) - p}{p - 1}\right] \tag{24}$$

Here, (η^1, η^2) are the dispersion matrix traces between the clusters and within the clusters, respectively, and (p) is the number of clusters. This centroid expresses a similar data distribution across the heterogeneous hospitals. Thus, the *vs* number of initialized centroids is represented as L. Subsequently, the ZD that combines the distribution similarity and geometric proximity is estimated. ZD ensures a more robust and adaptive measure of similarity.

This distance is measured between $(L)$and the gradient from the authenticated hospital $J^1[G(H)]$.

$$V = \sqrt{\sum r * \kappa\left(L - J^1[G(H)]\right)} * \left\{1 + \vartheta\left(L, J^1[G(H)]\right)\right\} \tag{25}$$

$$\vartheta = \frac{L * J^1[G(H)]}{\|L\| * \left\|J^1[G(H)]\right\|} \tag{26}$$

Where, $(V)$is the Zhonghua Distance between (L) and $J^1[G(H)]$, $(r, \kappa)$are the uniform feature weight and Huber loss, respectively, and (ϑ) is the cosine similarity between $(L)$and $J^1[G(H)]$. Next, the gradients are clustered regarding $(L)$and (V)as,

$$X = L * \min\left\{V\left\langle J^1[G(H)]\right\rangle\right\} \tag{27}$$

$$X \to \left[X\left(\left\langle J^1[G(H_1)]\right\rangle + \left\langle J^1[G(H_2)]\right\rangle + .. + \left\langle J^1[G(H_n)]\right\rangle\right)\right] \tag{28}$$

Here, $(X)$is the clustered output that indicates the aggregation of gradients from the heterogeneous hospitals, which is provided in equation (28). The cluster-wise aggregation continues until all the received gradients are clustered within the respective centroid. Further, the global prediction is done for analyzing the medical informatics aggregated from each local model.

3.3.2 Global Prediction

As explained in Section 3.1.2.6, the global CEP for each cluster is carried out based on (X) using MCN-GNN. The clustered data is considered as a node matrix, and the CEP is performed. Let the attained global prediction be represented as (Y). After attaining (Y), the global update is done in the distributed hospitals.

3.4 Distributed Hospitals

The distributed hospitals in the FL system are those connected via the main server. Here, the (n)number of heterogeneous hospitals is connected to the main server. Also, the prediction (Y) obtained in the global model is updated to each local model.

3.4.1 Continual Update

The updation of (Y) into hospitals (H) is performed using MEPDR. Regarding the avoidance of catastrophic forgetting, the Meta Experience Replay (MER) is utilized for continual updates. The MER stores a small buffer of past examples and mixes them with new data during update; hence, the model keeps “re-seeing” older tasks. Nevertheless, if replay samples are mostly from early tasks, then MER may overfit to those data and under-adapt to recent changes. Among various decay factors like Exponential Decay, Step Decay, and Polynomial Decay (PD) factor, the PD factor is selected because the Exponential and Step decay factors can cause abrupt learning-rate drops. PD diminishes the sampling probability, thereby ensuring that early-task samples don’t dominate the replay buffer and eliminating the overfitting issue. Further, by

integrating the PD factor, the proposed MEPDR dynamically balances the influence of past and recent tasks, thereby achieving robust gradient updates across tasks and improving continual learning performance in a federated environment.

Initially, the gradient (G) from the buffer samples of the local model and the new gradient (Y) from the global model are collected. The input of MEPDR (j) is expressed in equation (29) as,

$$j \to (G, Y) \tag{29}$$

Next, the PD $(\Re)$ that slows the decay of early samples is estimated to avoid the over-fitting issues and under-adaptation of the gradients by the local model.

$$\Re = \frac{1}{[1 + (\lambda * b)]^{\tau}} \tag{30}$$

Here, (λ) is the decay rate controlling factor, (τ) is the degree of polynomial decay that shapes the decay curve, and (b) is the total iteration. Further, $(\Re)$ is utilized to blend (G) and (Y) and form a weighted gradient (A).

$$A = (\Re * G) + [(1 - \Re) * Y] \tag{31}$$

This (A) is given to the authenticated local model $J^1[G(H)]$, and the precise CEP is carried out in the local model.

$$A \xrightarrow{\text{CEP}} J^1[G(H)] \tag{32}$$

Hence, the local model gradients are updated regarding old data present in the local model itself and the new data attained from the global model of the FL.

Pseudo-code for MEPDR

Input: Prediction (Y) and hospitals (H)
Output: Updation Outcomes

Begin
Initialize (Y) and (H)
For (Y)
Collect gradient (G) from the buffer samples of the local model and the new gradient (Y) from the global model
$j \to (G, Y)$
Compute PD
$\Re = \frac{1}{[1 + (\lambda * b)]^{\tau}}$
Blend (G) and (Y)
Form weighted gradient
$A = (\Re * G) + [(1 - \Re) * Y]$
Give (A) to the authenticated local model $J^1[G(H)]$
Estimate precise CEP

$$A \xrightarrow{\text{CEP}} J^{1}[G(H)]$$

Perform updation

End For

Obtain Updation Outcomes

End

Thus, the catastrophic forgetting is mitigated using MEPDR, which ensures that the local model relies on both the local data and the incoming global gradient. Next, all the transactions are stored in the blockchain.

3.5 Blockchain

Finally, the transactions (C) of the hospitals (H) regarding registration, login, local model CEP training, privacy preservation, hospital authentication, global aggregation, global prediction, and continual update are stored in the blockchain in the form of hash values (ζ). The blockchain is a distributed and immutable ledger technology, where every transaction is recorded in a block. Moreover, anyone in the network can verify the authenticity and order of updates without relying on a central authority.

$$C \to H(C) + \zeta \tag{33}$$

Thus, (C) is recorded in the blockchain. Once (C) is recorded, the updates can't be modified or deleted without consensus from network participants. This improves the fairness and accountability of the proposed system. Hence, the proposed model predicted the client event and ensured security via FL. The proposed framework's performance is explained in the subsequent section.

Code Availability

The code developed for this study is provided as Supplementary Material along with this manuscript. It includes the implementations of the proposed models and algorithms used in the experiments. The shared code corresponds to the version used to generate the reported results and is sufficient for reproducing the study. The code is available for academic and research use.

4. RESULTS AND DISCUSSION

Here, the performance analysis as well as comparison of the proposed techniques are carried out to prove the proposed model's effectiveness. The implementation is carried out on the working platform of PYTHON. Here, the experimental results are obtained by considering the average performance of the local models in the proposed federated learning scheme, illustrating that the proposed work is applicable for predicting diverse clinical events.

4.1 Experimental Setup

(a) Dataset Description

For the CEP in hospital 1, the "Heart Failure Prediction Dataset" that comprises the electronic health records of the patients is collected. Likewise, the "Stroke Prediction Dataset" is gathered from publicly available sources for the CEP in hospital 2. Also, for the CEP in hospital 3, the "Cirrhosis Prediction Dataset" is employed. Furthermore, the "Chronic Kidney Disease Dataset" is used for the CEP in hospital 4, whereas the "Diabetes Prediction Dataset" is applied for CEP in hospital 5. These dataset links are provided in the reference section. A total of 919 data are available to train the local model 1. Also, the "Stroke Prediction Dataset" consists of 5110 number of data to train the local model 2. Likewise, the "Cirrhosis Prediction Dataset" encompasses 418 numbers of data to train the local model 3. Similarly, "Chronic Kidney Disease Dataset" contains 400 numbers of data to train the local model 4, while the local model 5 is trained by using the "Diabetes Prediction Dataset", which includes 100000 numbers of data. The dataset specifications are provided in Table 1.

Table 1: Dataset Specifications

Dataset	Training (80%)	Testing (20%)	Total number of data
Heart Failure Prediction Dataset	735	184	919
Stroke Prediction Dataset	4088	1022	5110
Cirrhosis Prediction Dataset	334	84	418
Chronic Kidney Disease Dataset	320	80	400
Diabetes Prediction Dataset	80000	20000	100000

From that, 80% and 20% of the data are used for training and testing, respectively.

(b) Hyperparameter Details

Next, the hyperparameters used for the proposed algorithms are given in Table 2.

Table 2: Hyperparameters for the proposed algorithms

S.No	Parameters	Values
	Proposed MCN-GNN	
1	Optimizer	Adam
2	Initial learning rate	0.001
3	Activation function	ReLU

4	Number of GNN layers	2 to 4
5	Normalization method	MCN
6	Batch size	32
7	Number of training epochs	100
8	Loss function	Cross-entropy loss
	Proposed HRLSE	
1	Number of keys	4
2	Polynomial Modulus Degree	8192
3	Secret Key Size	256 bits
4	Ciphertext Size	~8–12 KB
5	Coefficient Modulus	[60, 40, 40, 60] bits
	TCG Construction	
1	Time window length	24–48 time steps
2	Temporal lag	1-3
3	Sliding window stride	1
4	Maximum temporal depth	5
5	Causality threshold	0.3–0.6
6	Minimum edge weight	0.05
7	Temporal smoothing factor	0.1-0.3
8	Edge pruning ratio	20-40%
	FL	
1	Federated rounds	100
2	Client participation ratio	0.3
3	Communication cost per round	84 MB
4	Uplink cost per round	72 MB
5	Downlink cost per round	12 MB
6	Mild Non-IID	0.5
7	Severe Non-IID	0.1
8	Data Size Sampling Variance	1.0

9	Client Sampling Ratio	0.3
10	Batch Size	32
11	Epochs per client	5
	Blockchain	
1	Blockchain type	Permissioned blockchain
2	Blockchain Platform	Hyperledger Fabric
3	Consensus Mechanism	Practical Byzantine Fault Tolerance (PBFT)
4	Network Participants	Hospitals, Client nodes, and Aggregation server
5	Peer Nodes	One for each hospital
6	Computational Overhead	Linear
7	Storage Overhead	Low
8	Gas Cost	0
9	Transaction Throughput	800–1200 tx/s
10	Storage per Transaction	0.5–1 KB

Table 2 displays the implementation details of the blockchain model. Here, the blockchain network had low computational overhead, low storage overhead, zero gas-cost, and high transaction throughput. Compared to other decentralized trust mechanisms (Decentralized Identifiers (DIDs) and Hashgraph), the blockchain network in the proposed model provided better auditability and storage due to its high trust level and validator selection.

(c) Mathematical Formulas

The mathematical formulas for the performance metrics used in the evaluation of the proposed method are depicted in Table 3.

Table 3: Mathematical formula for the performance metrics

Performance Metrics	**Formula**
Retained Accuracy	$\frac{1}{Tn-1}\sum_{s=1}^{Tn-1}\alpha_{Tn,s}$
Average Forgetting	$\frac{1}{Tn-1}\sum_{s=1}^{Tn-1}\left(max_{v<s}\,\alpha_{v,s}-\alpha_{Tn,s}\right)$

Forward Transfer	$\frac{1}{Tn-1}\sum_{s=2}^{Tn-1}\left(\alpha_{s-1,s}-\alpha_{0,s}\right)$
Backward Transfer	$\frac{1}{Tn-1}\sum_{s=1}^{Tn-1}\left(\alpha_{Tn,s}-\alpha_{s,s}\right)$
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
F-Measure	$2*\frac{precision\bullet recall}{precision+recall}$
PPV	$\frac{TP}{TP+FP}$
NPV	$\frac{TN}{TN+FN}$
FNR	$\frac{FN}{FN+TP}$
FPR	$\frac{FP}{FP+TN}$
MSE	$\frac{1}{N}\sum_{a=1}^{N}\left(Y_a-\tilde{Y}_a\right)^2$
MAE	$\frac{1}{N}\sum_{a=1}^{N}\left\|Y_a-\tilde{Y}_a\right\|$
Loss Convergence Rate	$\frac{Loss\ value\ end-Loss\ value\ start}{Communication\ rounds\ end-Communication\ rounds\ start}$
Jain's fairness index	$\frac{\left(\sum_{a=1}^{N}Y_a\right)^2}{N\sum_{a=1}^{N}Y_a^2}$
Security Level	$(W1\times K\%)+(W2\times C\%)+(W3\times E\%)+(W4\times P\%)+(W5\times I\%)$

Attack Level	$\frac{Number\ of\ successful\ attacks}{Total\ number\ of\ attacks}$
Encryption Time	$Encryption\ end\ time - Encryption\ start\ time$
Decryption Time	$Decryption\ end\ time - Decryption\ start\ time$
Signature Creation Time	$Signature\ creation\ end\ time - Signature\ creation\ start\ time$
Signature Verification Time	$Signature\ verification\ end\ time - Signature\ verification\ start\ time$
Clustering Time	$Clustering\ end\ time - Clustering\ start\ time$
Silhouette Score	$\frac{Int - Near}{max(Int, Near)}$
Davies–Bouldin Index	$\frac{1}{nC}\sum_{b=1}^{nC} \max_{c \neq b}\left(\frac{Cu_b + Cu_c}{Sp_{bc}}\right)$

Where, TP, TN, FN, and FP specify the true positive, true negative, false negative, and false positive, correspondingly, K specifies the key length contribution, C defines the attack complexity contribution, E denotes the encryption algorithm strength contribution, P exemplifies the privacy preservation contribution, I illustrates the implementation security contribution, N specifies the number of samples, Y_a denotes the actual value of the a^{th} sample, $\tilde{Y}_a$ indicates the predicted value of the a^{th} sample, Int illustrates average intra-cluster distance, $Near$ defines nearest cluster distance, Tn represents the number of tasks (s), $\alpha_{v,s}$ implies the accuracy at task s after learning task v, nC indicates the number of formed clusters, Cu_b and Cu_c exemplify intra-cluster scatter of cluster b and c, respectively, and Sp_{bc} defines inter-cluster separation.

4.2 Performance Evaluation

In this phase, the performance validation of the proposed methods, such as MEPDR, MCN-GNN, HRLSE, ExPrDSA, and CHIZD-KMC, is demonstrated to show the trustworthiness of each proposed model.

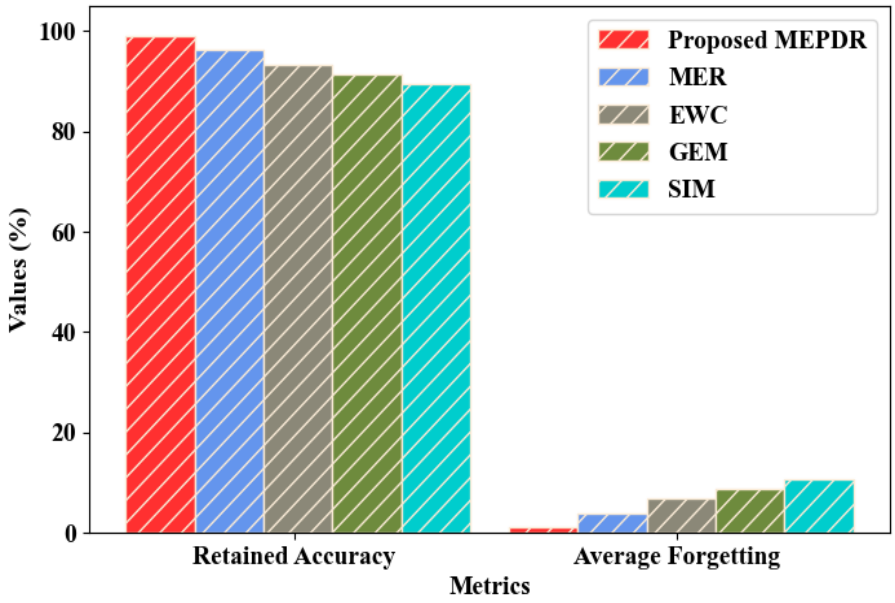


Figure 3: Comparative Analysis of MEPDR

Figure 3 illustrates the comparison of the proposed MEPDR and the prevailing methods like MER, Elastic Weight Consolidation (EWC), Gradient Episodic Memory (GEM), and Synaptic Intelligence Method (SIM) regarding continual update in the local model. The proposed MEPDR attained a retained accuracy of 98.95% and an average forgetting of 1.05%. However, the prevailing MER, EWC, GEM, and SIM attained retained accuracy values of 96.21%, 93.28%, 91.32%, and 89.47% and average forgetting values of 3.79%, 6.72%, 8.68%, and 10.53%, respectively. Thus, the integration of the gradient with the local model and the global update using PD improved the performance of the proposed method via continual update. PD excellently avoided the overfitting issue and under-adapted to recent changes. Therefore, the efficacy of the proposed methodology was proved.

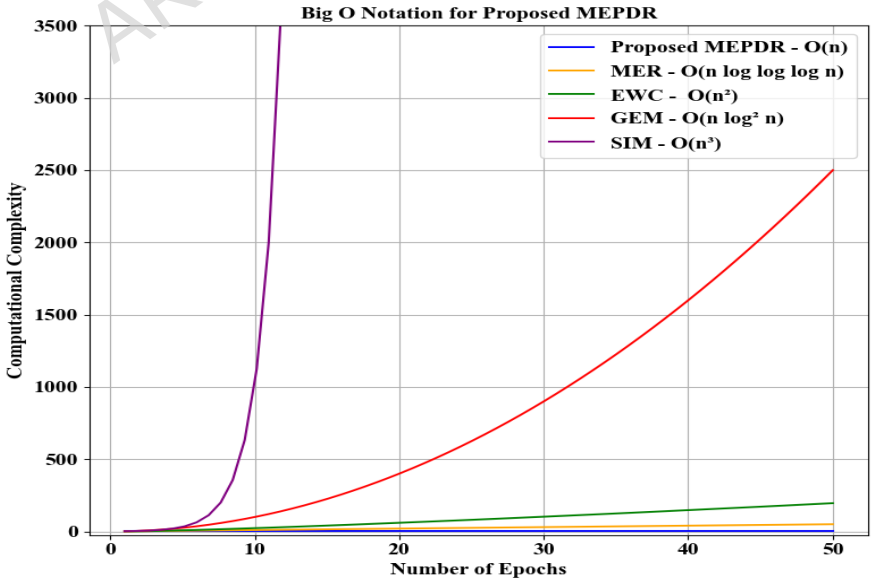


Figure 4: Computational complexity analysis

Figure 4 depicts the computational complexity investigation (Big O) of the proposed MEPDR and conventional techniques. A computational cost measures the resources that an algorithm or task consumes to assess the efficiency. The proposed MEPDR had a high computational complexity of O(n) owing to the usage of PD. But, the prevailing MER, EWC, GEM, and SIM attained low computational complexities. Hence, the proposed model outperformed prevailing methods.

Table 4: Comparative Analysis for LM 1

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
Proposed MCN-GNN	98.97	98.75	98.62	98.11
GNN	95.32	95.13	94.83	94.02
TCN	91.65	90.45	89.47	89.05
GRU	87.91	86.43	85.15	84.32
LSTM	83.28	82.94	82.38	81.94
LR	79.34	79.21	79.02	79.15
XGBoost	76.67	76.53	76.39	76.46

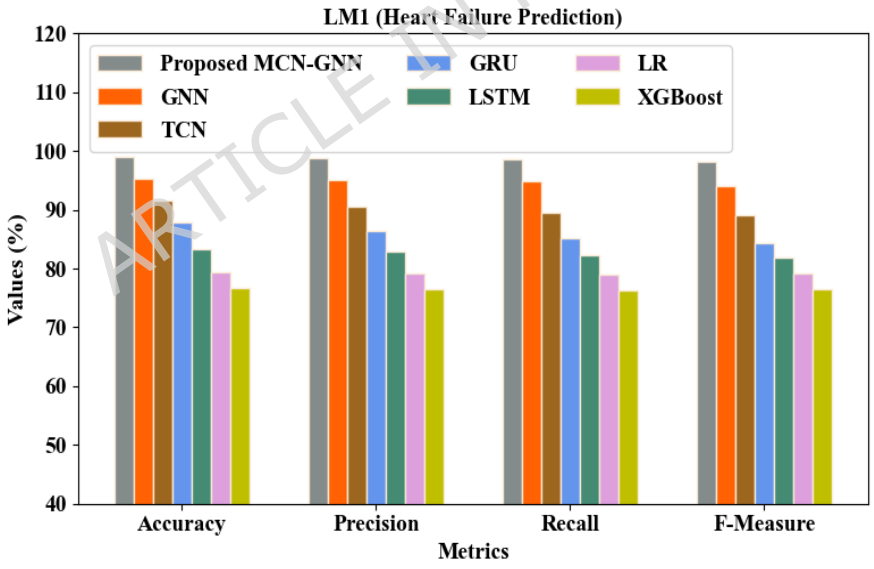


Figure 5: Graphical Comparison for Heart Failure Prediction

The proposed classifier distinguished the complex nodes using the MCN, which effectively prevented the over-smoothing issue. Also, the features from the pre-processed electronic health record and the TCG were fed into the proposed MCN-GNN as a node matrix. As given in Table 4 and Figure 5, heart failure was predicted in LM 1 with an accuracy of 98.97%, precision of 98.75%, recall of 98.62%, and F-Measure of 98.11%. But, the existing GNN, Temporal Convolutional Network (TCN), Gated Recurrent Unit (GRU), LSTM, Logistic Regression (LR), and eXtreme Gradient Boosting (XGBoost) achieved accuracy values of 95.32%,

91.65%, 87.91%, 83.28%, 79.34%, and 76.67%, precision values of 95.13%, 90.45%, 86.43%, 82.94%, 79.21%, and 76.53%, recall values of 94.83%, 89.47%, 85.15%, 82.38%, 79.02%, and 76.39%, and F-Measure values of 94.02%, 89.05%, 84.32%, 81.94%, 79.15%, and 76.46%, correspondingly. This showed that the proposed classifier predicted the heart failure event better than the existing classifiers.

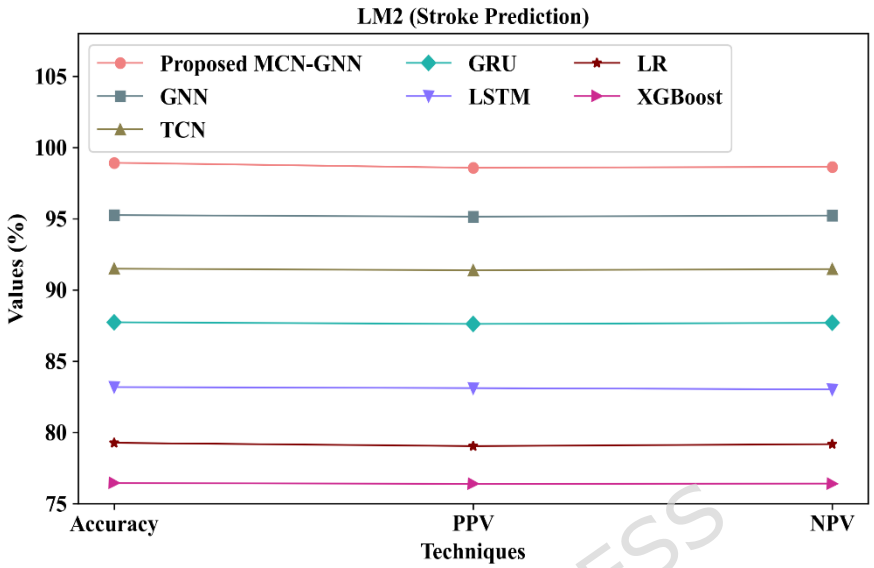
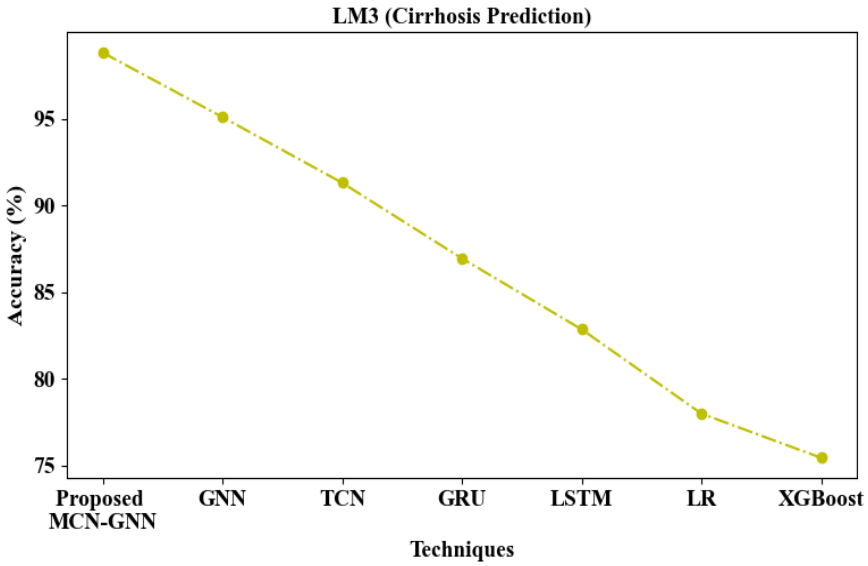
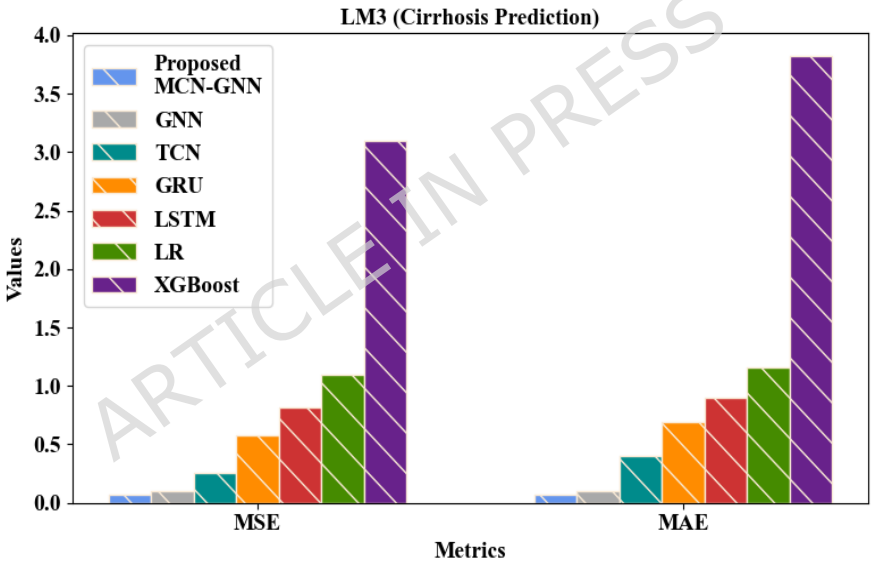


Figure 6: Pictorial representation for LM 2 regarding stroke prediction

Figure 6 illustrates the pictorial representation of the proposed MCN-GNN and existing techniques concerning accuracy, Positive Predictive Value (PPV), and Negative Predictive Value (NPV). The proposed method attained high accuracy, PPV, and NPV of 98.92%, 98.57%, and 98.64% for stroke prediction in Local Model 2, respectively. However, the prevailing GNN and LSTM attained low accuracy values of 95.25% and 83.18%, correspondingly. Also, the prevailing GRU and LR obtained low PPVs of 87.61% and 79.04%, respectively. Likewise, the conventional TCN and XGBoost attained low NPVs of 91.46% and 76.41%, correspondingly. Here, the proposed model showed improved performance owing to the usage of MCN, which prevented over-smoothing and improved robustness in stroke prediction (LM 2). Thus, the effectiveness of the proposed method was proved.



(a)



(b)

Figure 7: Performance evaluation of cirrhosis prediction for the proposed MCN-GNN in LM3 regarding (a) accuracy and (b) MSE and MAE

Figure 7 (a) and (b) depict the performance assessment of the proposed MCN-GNN and existing methodologies for LM 3 (cirrhosis prediction). Here, MCN was employed between the layers of GNN to prevent over-smoothing and reduce the extra feature averaging. For LM 3 (cirrhosis prediction), the proposed MCN-GNN achieved a high accuracy (98.83%) and low MSE (0.06471) and MAE (0.07164). But, the prevailing GNN, TCN, GRU, LSTM, LR, and XGBoost attained an average accuracy, MSE, and MAE of 84.955%, 0.989955, and 1.177543, respectively, which were poorer than the proposed method. Thus, the analysis proved that the proposed method accurately predicted the cirrhosis disease in LM 3.

Table 5: Comparative Analysis of HRLSE

Methods	Security Level (%)	Attack Level (%)	Encryption Time (ms)	Decryption Time (ms)
Proposed HRLSE	98.85	1.15	4021	4214
HE	95.52	4.48	7945	8203
ECC	92.21	7.79	10463	11237
RSA	89.38	10.62	14032	14472
AES	88.04	11.96	17832	18932

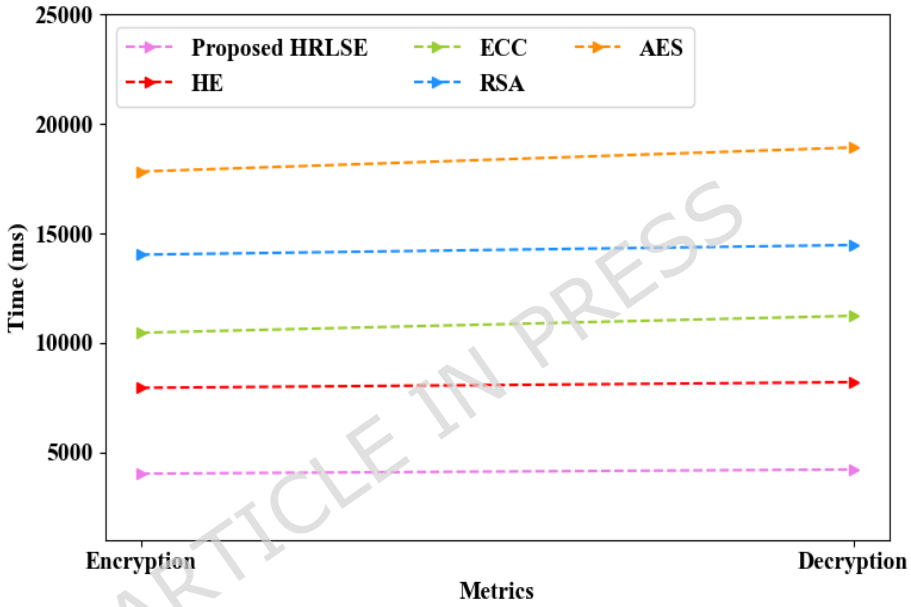


Figure 8: Graphical Comparison of HRLSE

The performance validation of the proposed HRLSE and the existing methodologies regarding privacy preservation of the local model's gradients is depicted in Table 5 and Figure 8. The proposed HRLSE and the traditional HE, Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), and Advanced Encryption Standard (AES) secured the local model's gradient with security levels of 98.85%, 95.52%, 92.21%, 89.38%, and 88.04%, attack levels of 1.15%, 4.48%, 7.79%, 10.62%, and 11.96%, encryption times of 4021ms, 7945ms, 10463ms, 14032ms, and 17832ms, and decryption times of 4214ms, 8203ms, 11237ms, 14472ms, and 18932ms, correspondingly. In HRLSE, RLS effectively avoided the noise growth produced by continual homomorphic additions and multiplications. Hence, the avoidance of noise amplification using RLS in the proposed model enhanced the privacy preservation of the gradients compared to the conventional techniques.

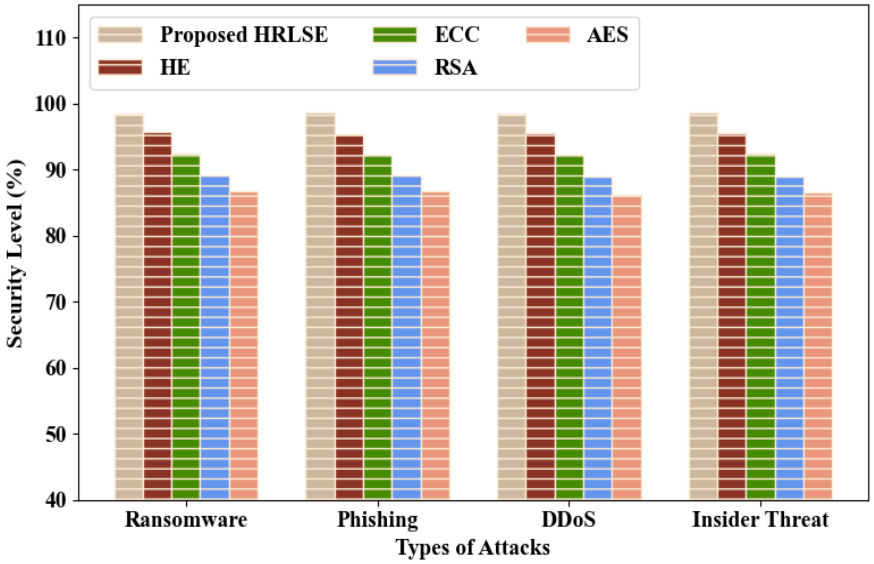


Figure 9: Security level evaluation for different types of attacks

Figure 9 depicts the security level evaluation of the proposed HRLSE and traditional techniques for different types of attacks. Here, the proposed HRLSE employed RLS for avoiding the noise amplification. The proposed HRLSE achieved high security levels of 98.54%, 98.71%, 98.49%, and 98.69% for ransomware, phishing, Distributed Denial of Service (DDoS), and insider threat attacks, respectively. However, the prevailing HE, ECC, RSA, and AES achieved low average security levels of 91%, 90.86%, 90.71%, and 90.87% for different types of attacks, correspondingly. Thus, the proposed model attained improved performance across different attack scenarios.

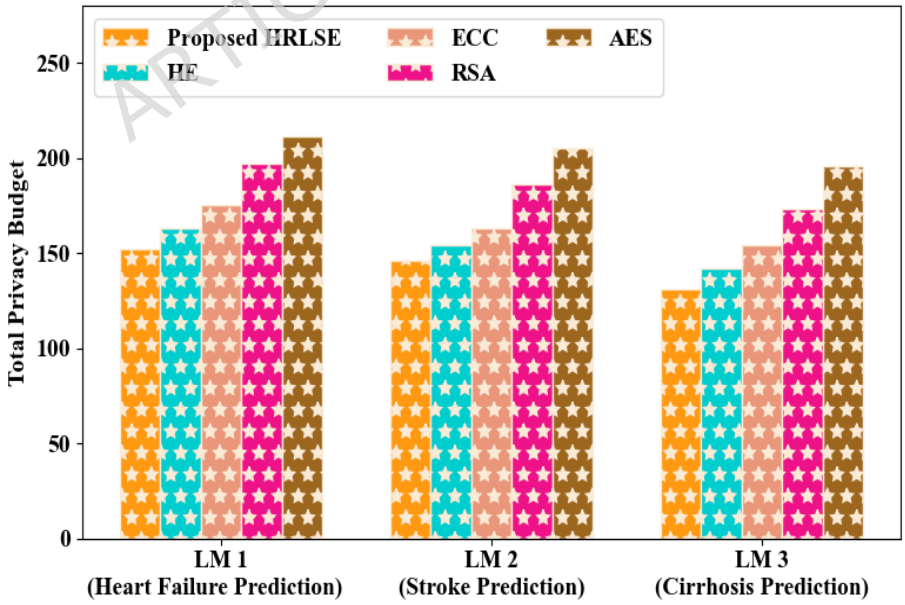


Figure 10: Differential Privacy Budget Analysis of the Proposed HRLSE

From Figure 10, it was proven that the proposed HRLSE effectively maintained a controlled differential privacy budget, ensuring that the local model gradients were securely encrypted

while limiting the cumulative privacy loss. As a result, the proposed HRLSE demonstrated an appropriate and low privacy budget during model gradient privacy preservation. Therefore, the proposed HRLSE precisely protected model gradients without significantly affecting the model performance, making it appropriate for privacy-preserving federated learning in clinical environments.

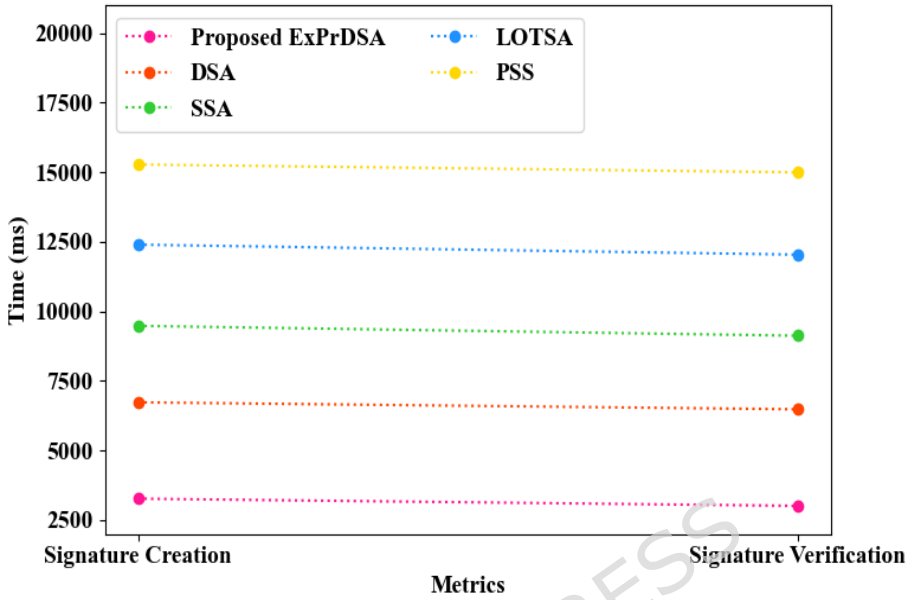


Figure 11: Graphical Comparison of ExPrDSA

The comparison of the proposed ExPrDSA and the prevailing methods regarding hospital authentication is illustrated in Figure 11. The proposed model generated the hash function for digital signature creation using ExPr, which made collision prediction harder and improved the robustness against hash-flooding attacks. Thus, the hospital was authenticated with a Signature Creation Time (SCT) of 3271ms and Signature Verification Time (SVT) of 3012ms. However, the prevailing DSA, Schnorr Signature Algorithm (SSA), Lamport One-Time Signature Algorithm (LOTSA), and Probabilistic Signature Scheme (PSS) obtained SCTs of 6732ms, 9478ms, 12395ms, and 15273ms and SVTs of 6481ms, 9123ms, 12036ms, and 14992ms, respectively. Therefore, the outcomes depicted that the proposed ExPrDSA authenticated the hospitals better than the traditional methods.

Table 6: Comparative Analysis of CHIZD-KMC

Techniques	Clustering Time (ms)	Silhouette Score	Davies–Bouldin Index
Proposed CHIZD-KMC	4342	0.9312	2.33
KMC	8942	0.9091	5.39
CLARA	12382	0.8875	9.94
PAM	16734	0.8501	15.38
FCM	20489	0.7945	22.38

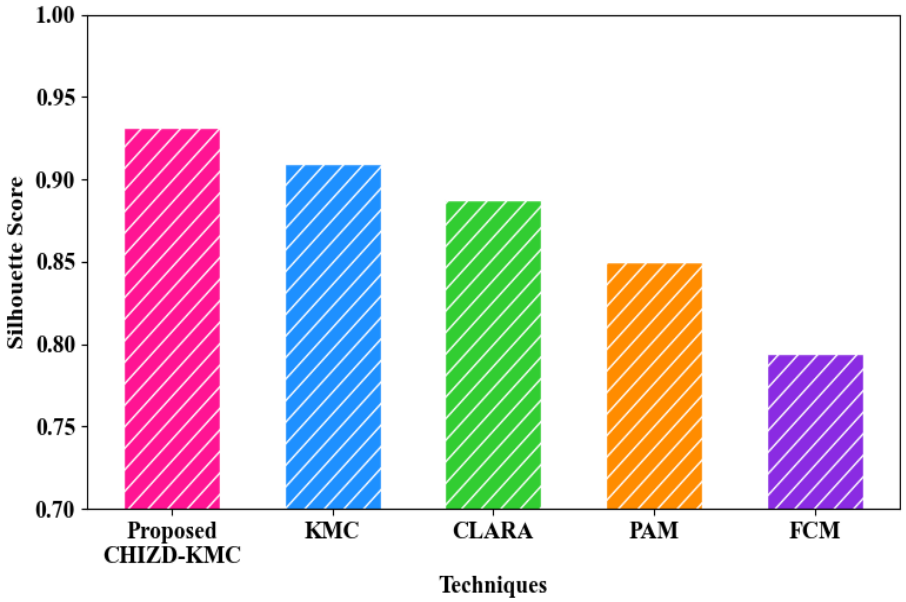


Figure 12: Graphical Comparison regarding Silhouette Score

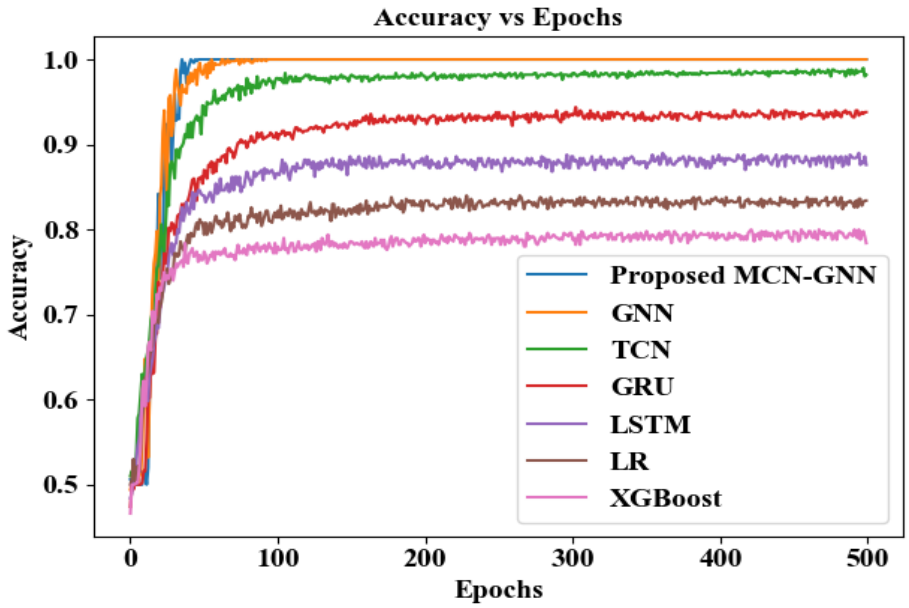
The comparison of the proposed CHIZD-KMC and the traditional models regarding cluster-wise aggregation in the global model is given in Table 6 and Figure 12. The proposed model aggregated the gradients with a clustering time of 4342ms, a silhouette score of 0.9312, and a Davies–Bouldin Index (DBI) of 2.33. On the other hand, the prevailing KMC, Clustering Large Applications (CLARA), Partition Around Medoids (PAM), and Fuzzy C-Means (FCM) aggregated the gradients with clustering times of 8942ms, 12382ms, 16734ms, and 20489ms, silhouette scores of 0.9091, 0.8875, 0.8501, and 0.7945, and DBIs of 5.39, 9.94, 15.38, and 22.38, respectively. Thus, the generation of the centroid using CHI and the utilization of Zhonghua Distance in the proposed model enhanced the cluster-wise aggregation over existing models.

Table 7: Performance Assessment for FL

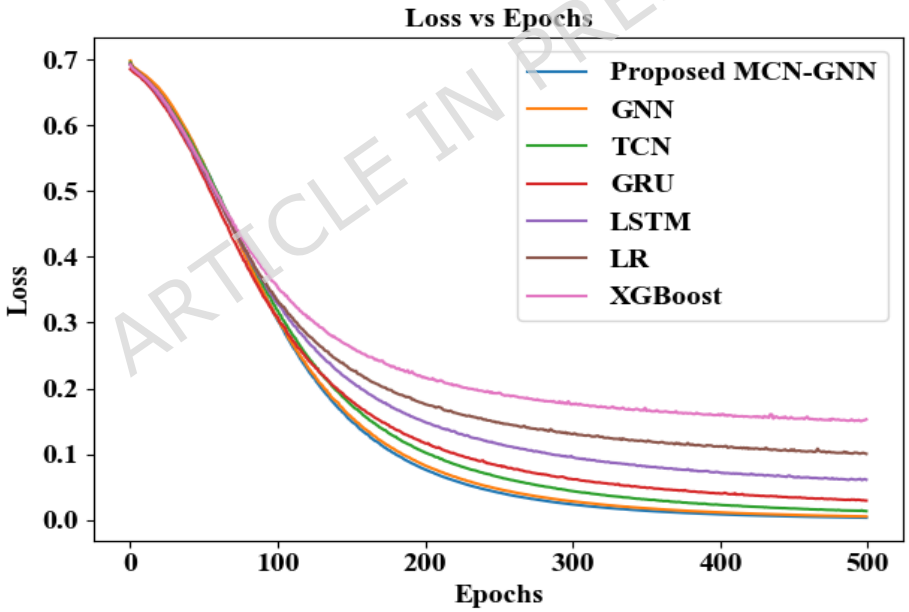
Techniques	Loss Convergence Rate	Jain's Fairness Index
Proposed HFL-based CHIZD-KMC	-0.035	0.95
FedDyn	-0.029	0.89
SCAFFOLD	-0.026	0.84
FedNova	-0.022	0.76
FedProx	-0.017	0.71
FedAvg	-0.013	0.63

Table 7 displays the performance assessment of the proposed Horizontal Federated Learning (HFL)-based CHIZD-KMC and prevailing FedDyn, SCAFFOLD, FedNova, FedProx, and FedAvg. Here, the proposed HFL-based CHIZD-KMC achieved a high loss convergence rate (-0.035) and Jain's fairness index (0.95), where HFL with CHI and ZD elevated the aggregation performance. However, the prevailing FedDyn, SCAFFOLD, and FedNova attained low loss convergence rates of -0.029, -0.026, and -0.022, correspondingly. Also, the existing FedProx and FedAvg attained low Jain's fairness index values of 0.71 and 0.63, respectively. The proposed model attained improved performance, showing the effectiveness of realistic multi-

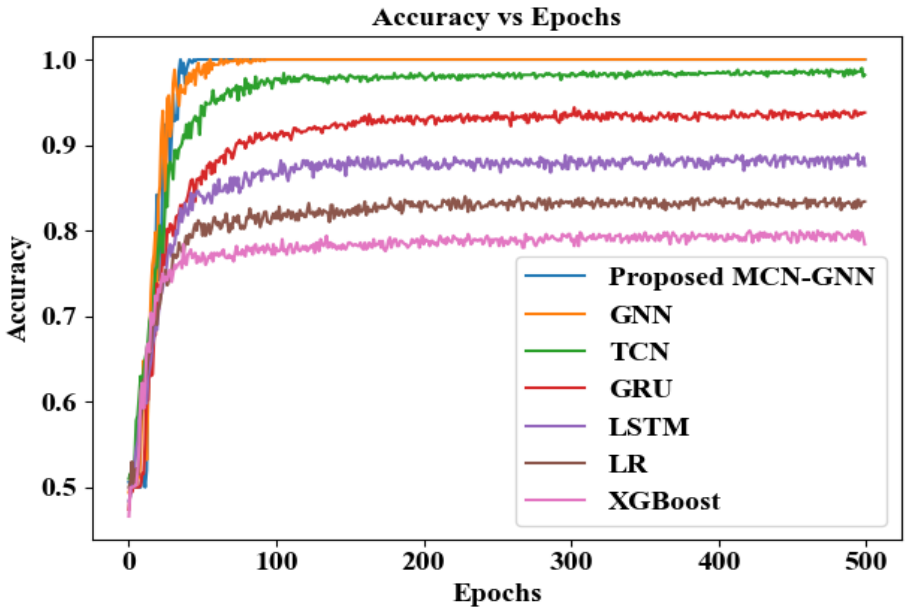
client FL. Thus, the proposed model excellently performed cluster-wise aggregation of the gradient related to different disease diagnosis outputs from various authenticated hospitals.



(a)



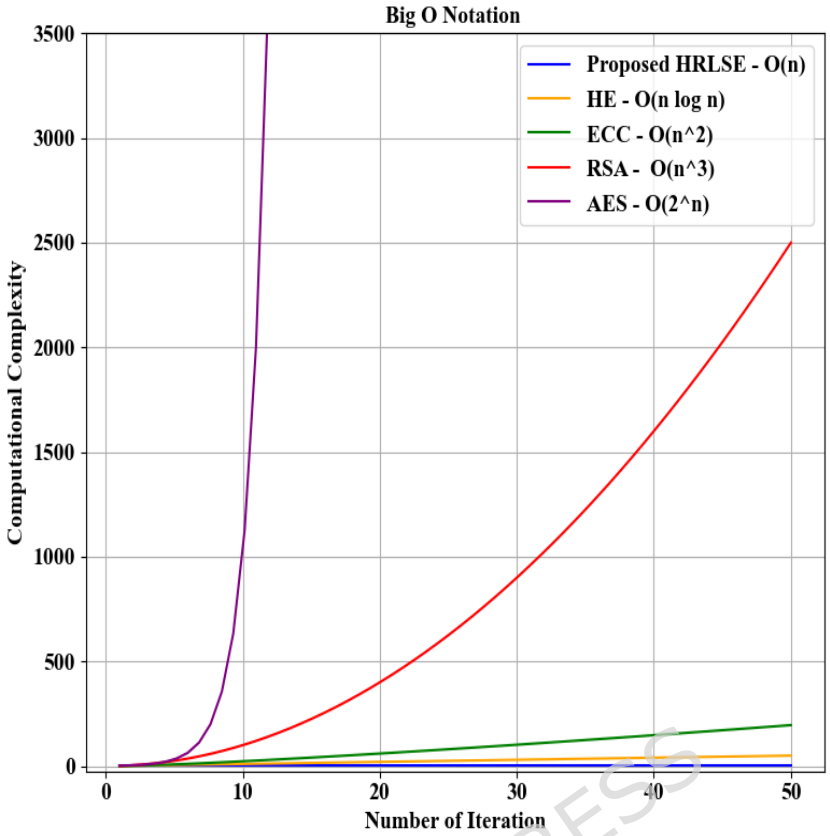
(b)



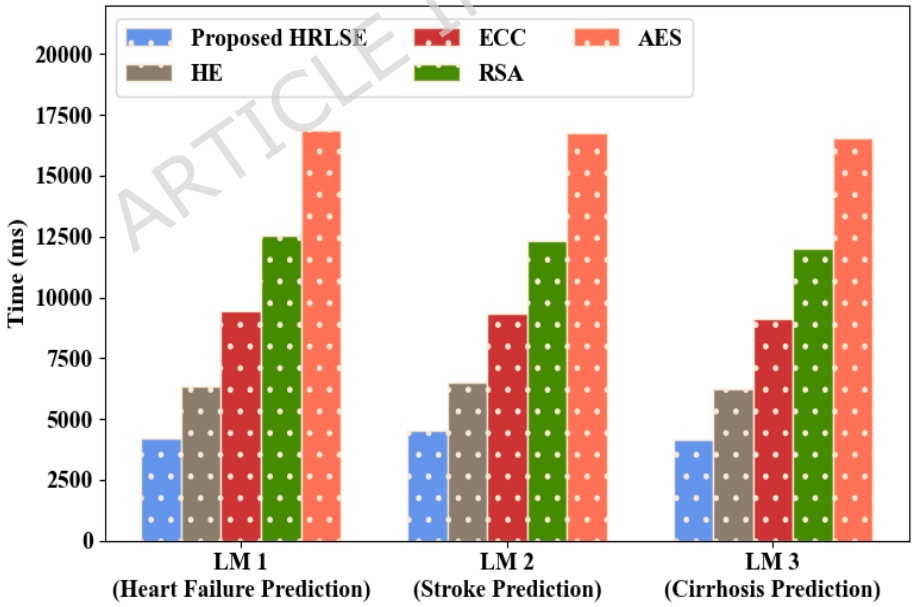
(c)

Figure 13 (a), (b), and (c): Performance Analysis of the proposed MCN-GNN regarding Global Accuracy, Convergence Curves, and communication costs per-round/epochs

As per Figures 13(a), (b), and (c), the proposed MCN-GNN achieved higher global accuracy, faster convergence, and lower communication cost per round during federated learning training. As a result, the proposed MCN-GNN consistently attained superior accuracy even at a higher number of communication rounds than the traditional methods. Similarly, the proposed MCN-GNN significantly reduced communication overhead at varying numbers of rounds, making it efficient for large-scale federated learning environments. Also, the proposed MCN-GNN demonstrated rapid and stable convergence across training rounds/epochs. Therefore, the proposed work ensured scalability in real-world clinical event prediction.



(a)



(b)

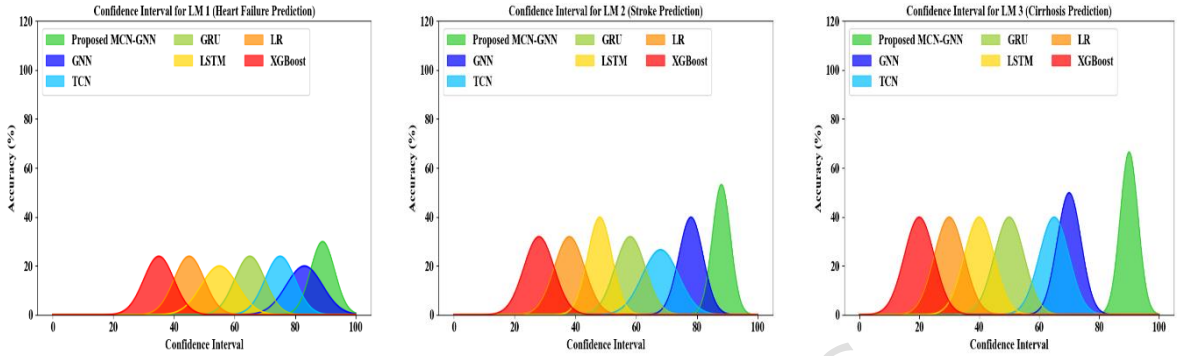
Figure 14 (a) and (b): Computational Complexity and Communication Overhead Analysis of the FL+ HRLSE+Blockchain

Figures 14(a) and (b) displayed that as the number of participating hospitals and training rounds increased, the computational complexity and communication overhead of the proposed

FL+HRLSE+Blockchain framework remained manageable and scalable. Although the integration of security and blockchain introduced additional processing steps, the overall complexity increased in a controlled and non-linear manner, demonstrating that the framework was suitable for practical, large-scale federated learning deployments requiring excessive computational overhead.

4.3 Empirical Assessment of the Local Models (LM1, LM2, and LM3)

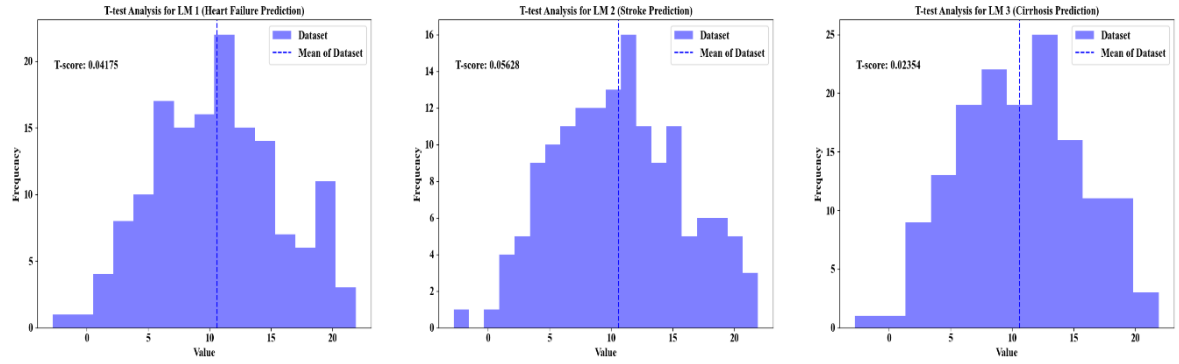
In this phase, the proposed framework's effectiveness is validated under LM1, LM2, and LM3.



(a) (b) (c)

Figure 15: Confidence Interval Analysis for (a) LM1, (b) LM2, and (c) LM3

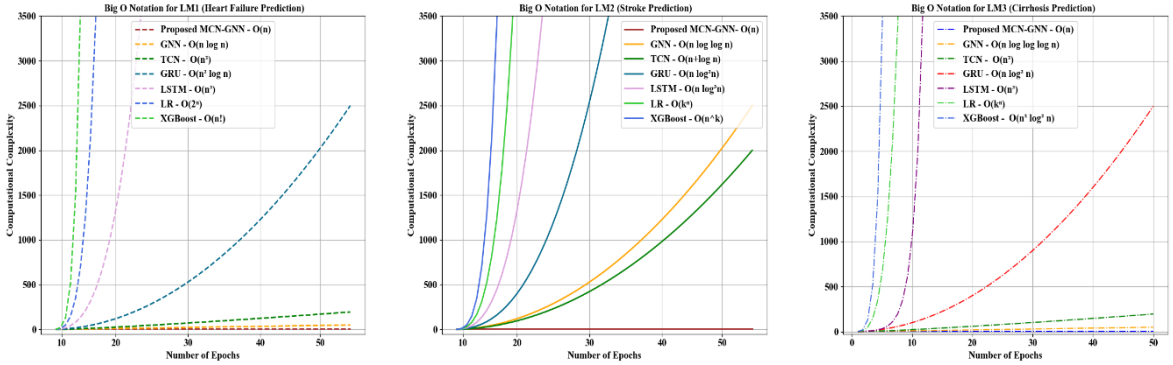
Confidence interval analysis of the proposed MCN-GNN and conventional methods for LM1, LM2, and LM3 is depicted in Figure 15. In general, a confidence interval visually indicates the statistical estimate that specifies the accuracy distributions across training epochs. It shows how the accuracy of the model differs with its peak value. Also, the confidence interval graph revealed an explicit uncertainty estimate by showing the prediction variability around accuracy. The proposed MCN-GNN had enhanced performance for CEP due to the usage of MCN-based normalization. But, the prevailing techniques attained limited performance.



(a) (b) (c)

Figure 16: T-test validation for (a) LM1, (b) LM2, and (c) LM3

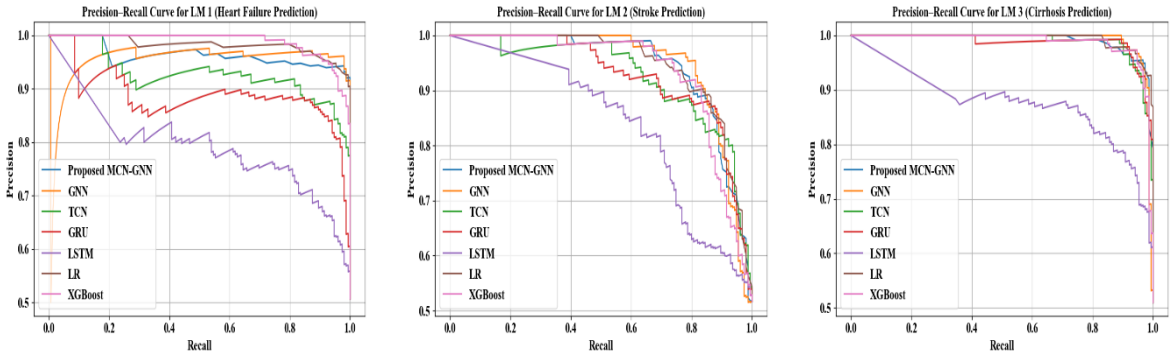
Figure 16 shows the t-test validation for LM1, LM2, and LM3 of the proposed method. Here, based on the histogram of dataset values, the outcomes of a t-test validation are presented. The T-test measures the standardized difference betwixt the sample mean and the expected mean. In Figure 16, the x-axis specifies the value range and the y-axis illustrates the frequency of observations. Also, the distribution of histogram values is displayed in the histogram bars. The reference point is marked by a dashed vertical line. Here, the proposed model has a t-test value of 0.04175, 0.05628, and 0.02354 for LM1, LM2, and LM3, respectively. Thus, the significance test shows the effectiveness of the proposed model.



(a) (b) (c)

Figure 17: Big O Complexity Analysis of proposed MCN-GNN for (a) LM1, (b) LM2, and (c) LM3

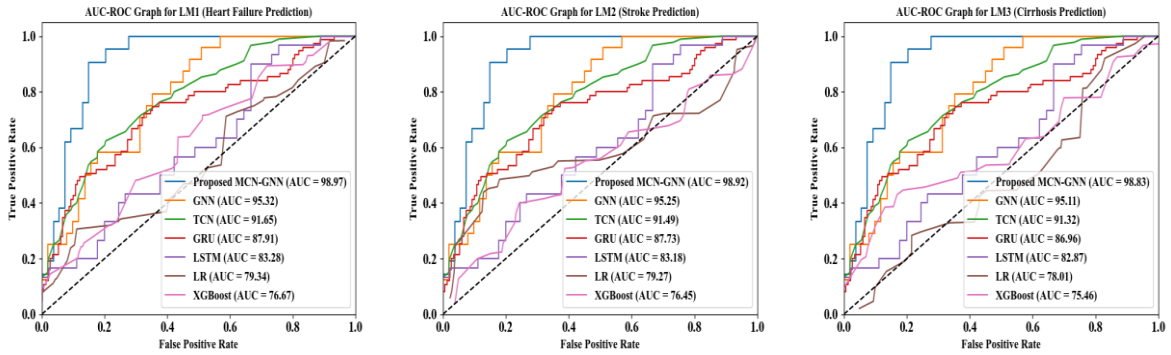
Big O complexity investigation of the proposed MCN-GNN and prevailing models for LM1, LM2, and LM3 is displayed in Figure 17. Normally, Big O notation indicates the efficiency of an algorithm in time by showcasing its performance with input size. For LM1, LM2, and LM3, the proposed MCN-GNN achieved a low computational complexity of O(n) owing to the usage of MCN. Yet, the prevailing GNN, TCN, GRU, LSTM, LR, and XGBoost attained high computational complexity for all local models. Hence, the proposed model was better than the existing methodologies.



(a) (b) (c)

Figure 18: Precision Recall Curve Analysis for (a) LM1, (b) LM2, and (c) LM3

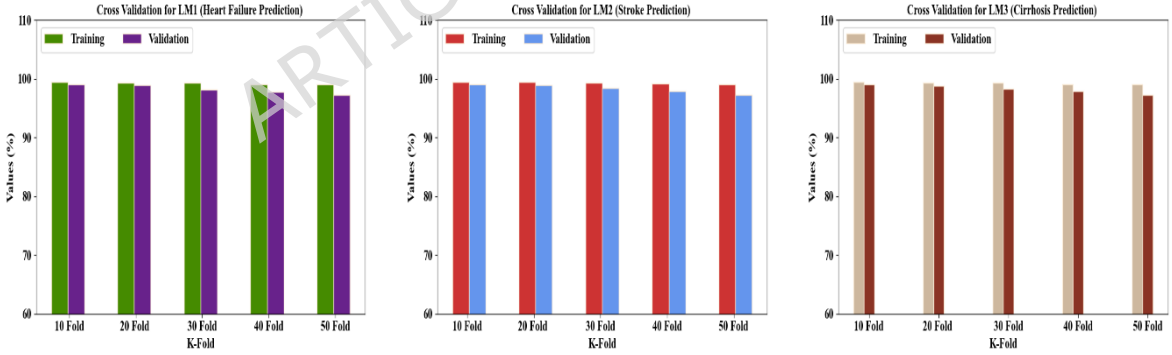
Figure 18 displays the precision-recall curve investigation of the proposed MCN-GNN and conventional models for LM1, LM2, and LM3. Here, the PR curve exemplifies how the precision and recall change at each step. A higher precision-recall curve specifies a strong and reliable prediction performance. Thus, the analysis showed that the proposed model was superior to the existing methods. Also, the MCN-based normalization was employed between the layers of GNN, thus preventing the over-smoothing issue.



(a) (b) (c)

Figure 19: AUC-ROC curve validation for (a) LM1, (b) LM2, and (c) LM3

Area Under the Curve-Receiver Operating Characteristics (AUC-ROC) analysis of the proposed model and prevailing techniques for LM1, LM2, and LM3 is displayed in Figure 19. In the AUC-ROC curve, the higher values represent that the model superiorly predicted the diseases. The proposed model had higher AUC-ROC curve values owing to the usage of MCN. Thus, the reliability of the proposed model was demonstrated.



(a) (b) (c)

Figure 20: Cross-Validation analysis for (a) LM1, (b) LM2, and (c) LM3

Figure 20 depicts the cross-validation investigation of the proposed method for LM1, LM2, and LM3. In general, cross-validation models the predictive value of a statistical model by dividing a dataset into training and testing sets, thus excellently evaluating the performance of the model. For LM1, the proposed model achieved training accuracies of 99.4587% (10 fold), 99.3568% (20 fold), 99.2874% (30 fold), 99.1025% (40 fold), and 99.0254% (50 fold), and validation accuracies of 99.1054% (10 fold), 98.97% (20 fold), 98.1254% (30 fold), 97.8423

(40 fold), and 97.2572% (50 fold), thus proving the effective performance trend across all K-fold splits. Also, the proposed model attained better accuracy regarding training and validation for LM2 and LM3. Overall, the cross-validation revealed the overfitting avoidance and generalizability of the proposed model.

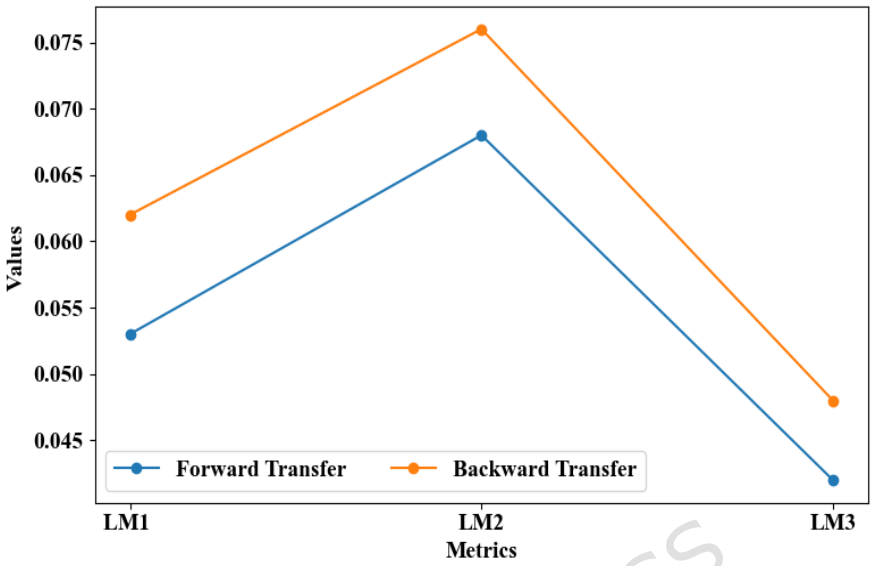


Figure 21: MEPDR evaluation on CL scenario with forgetting metrics

Figure 21 displays the MEPDR evaluation of the proposed model on the CL scenario with respect to forgetting metrics like forward transfer and backward transfer. Here, the PD was modified in MEPDR to avoid the overfitting issues, thus improving the continual update performance. For local model 3, the proposed model had low Forward Transfer (0.042) and Backward Transfer (0.048), which were higher compared to other local models because LM3 consisted of a huge amount of training data. For local models 2 and 1, the proposed model had high forward transfer values of 0.068 and 0.053 and high backward transfer values of 0.076 and 0.062, correspondingly. Thus, the trustworthiness of the proposed model was demonstrated.

Table 8: Robustness Analysis of the Proposed HRLSE under varying adversarial attacks regarding security level

Proposed Models	Adversarial Attacks/Security Level (%)	
	Evasion Attack	Poisoning Attack
LM1	98.83	98.82
LM2	98.8	98.81
LM3	98.84	98.8

As per Table 8, the proposed models (LM1, LM2, and LM3) demonstrated high robustness under both evasion and poisoning attacks, achieving security levels above 98.8%. This achievement indicated that the proposed HRLSE effectively resisted the adversarial

manipulations while preserving the integrity of model gradients and ensuring reliable learning even in hostile environments. Therefore, the proposed work showed significantly higher security levels across different local models against various adversarial threats.

Table 9: Calibration Analysis of the Proposed Models (LM1, LM2, and LM3)

Proposed Models	Accuracy (%)	MSE	RMSE
LM1	98.97	0.985579	0.99276
LM2	98.92	0.978922	0.9894
LM3	98.83	0.989955	0.99496

From Table 9, it was proven that the proposed models (LM1, LM2, and LM3) achieved high accuracy with very low error values, indicating strong calibration performance. Additionally, all their local models maintained higher accuracies and reduced errors, demonstrating that the predicted probabilities were well-aligned with the actual outcomes. Therefore, the proposed work produced accurate predictions while ensuring reliable and stable probability estimates in federated learning environments.

4.4 Ablation Study Analysis

Here, the ablation study is carried out for the proposed CHIZD-KMC.

Table 10: Ablation study for proposed CHIZD-KMC

Techniques	Sihoutte Score
Proposed model with CHI and ZD	0.9312
Proposed model without CHI	0.8957
Proposed model without ZD	0.8671

Table 10 depicts the ablation study for the proposed CHIZD-KMC. Here, the proposed model with CHI and ZD attained a high silhouette score of 0.9312, where CHI superiorly initialized the centroids and ZD avoided suboptimal clustering. But, the proposed model without CHI attained a low silhouette score of 0.8957, whereas the proposed model without ZD obtained a very low silhouette score of 0.8671. Thus, the proposed CHIZD-KMC was better for cluster-wise aggregation in FL, which improved the FL convergence and stability.

4.5 Subjective Assessment

In this phase, the proposed framework's qualitative test assessment is done under various subjects during clinical event prediction.

Table 11: Qualitative test assessment

Subjects	Evaluation scenario	Operational Condition	Model reliability	Privacy assurance	Computational overhead	System usability

Subject 1	Multi-hospital collaboration	Normal	4	4	3	4
Subject 2	Non-IID Data Distribution	Heterogeneous patient data	3	4	3	3
Subject 3	Continual data updation	More clinical updates	4	3	2	4
Subject 4	Threat Environment	Adversarial update attempts	3	4	2	3

Table 11 displays the qualitative test assessment for the proposed model in multiple evaluation scenarios and operational conditions. This validation is done for measuring the perceptual quality of the proposed model. Here, the feedback is provided in four scales, like 4 (excellent), 3 (good), 2 (moderate), and 1 (poor), for assessing the model's performance. According to different evaluation scenarios and operational conditions, the model's reliability, privacy assurance, computational overhead, and system usability show the robustness of the model.

4.6 Generalizability Analysis through LM4 and LM5

Here, the proposed work is evaluated under LM4 and LM5 to enhance the model's reliability in diverse clinical event prediction.

Table 12: Performance Analysis of the proposed work under Chronic Kidney Disease Dataset (LM4)

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
Proposed MCN-GNN	98.96	98.74	98.63	98.1
GNN	95.31	95.12	94.84	94
TCN	91.5	90.5	89.46	89
GRU	87.92	86.43	85.16	84.3
LSTM	83.29	82.95	82.39	81.95
LR	79.35	79.22	79.03	79.16
XGBoost	76.68	76.534	76.4	76.47

From Table 12, it was proven that the proposed MCN-GNN effectively performed clinical event prediction using the chronic kidney disease dataset compared to traditional models. As a result, the proposed MCN-GNN achieved 98.96% accuracy, 98.74% precision, 98.63% recall, and 98.1% f-measure, demonstrating its strong ability to accurately identify and classify clinical events. However, the traditional methods, such as GNN, TCN, GRU, LSTM, LR, and XGBoost, showed comparatively lower performance in chronic kidney disease prediction due

to the limited ability to capture high-order temporal-causal dependencies. Thus, by incorporating the MCN with traditional GNN, the proposed work enabled robust feature representation and improved predictive reliability in distributed clinical environments.

Table 13: Effectiveness Evaluation of the proposed work under the Diabetic prediction Dataset (LM5)

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
Proposed MCN-GNN	98.98	98.76	98.63	98.12
GNN	95.31	95.12	94.82	94.01
TCN	91.64	90.44	89.46	89.06
GRU	87.90	86.42	85.14	84.33
LSTM	83.27	82.96	82.37	81.93
LR	79.33	79.22	79.03	79.16
XGBoost	76.66	76.54	76.38	76.45

As per Table 13, the traditional methods demonstrated comparatively lower performance in clinical event prediction using the diabetic prediction dataset than the proposed MCN-GNN. For instance, the traditional GNN attained very low accuracy (95.31%), precision (95.12%), recall (94.82%), and f-measure (94.01%) due to the over-smoothing issue and limited capability to model long-range temporal-causal dependencies in heterogeneous EHR data. In contrast, the proposed MCN-GNN demonstrated superior performance by attaining higher accuracy, precision, recall, and f-measure values of 98.98%, 98.76%, 98.63%, and 98.12%, respectively. This depicted reliable and generalizable clinical event prediction in federated and heterogeneous healthcare environments.

4.7 Comparative Analysis

In this phase, the comparative analysis of the proposed work and traditional works is carried out.

Table 14: Existing Works Comparison

Study	Methods	Accuracy (%)	Recall (%)	F-Measure (%)	Precision (%)
Proposed Work	MCN-GNN	98.97	98.62	98.11	98.75
[30]	HarmoSATE	74	-	75	-
[31]	BFL	92.6	-	-	-
[32]	Multi-layer GNN	84.4	73.1	72.3	-

[33]	RDBN	92	91	92	-
[34]	EDBN	95.07	96.54	95.98	95.44

Table 14 describes the comparison of the proposed system and the existing works concerning CEP. The existing works used classifiers, such as Harmo Self-Attentive Encoder (HarmoSATE), Blockchain-enabled Federated Learning (BFL), Multi-layer GNN, Residual learning-centric Deep Belief Network (RDBN), and Entropy Deep Belief Network (EDBN), for clinical event prediction. In the proposed framework, the electronic health record was pre-processed, and the TCG was constructed. Further, the FL-based MCN-GNN was utilized for clinical event prediction, thus attaining an accuracy of 98.97%, a recall of 98.62%, an F-Measure of 98.11%, and a precision of 98.75%. However, the existing [30-32] predicted the client event without analyzing the cause and effect between the features, thereby attaining accuracy values of 74%, 92.6%, and 84.4%, respectively. Also, the prevailing [33, 34] couldn't capture the temporal dependencies, thus attaining lower accuracy, recall, precision, and F-Measure values than the proposed work. When contrasted with the prevailing works, the proposed work improved the CEP.

Clinical Relevance Evaluation

In real-world clinical settings, the proposed model offers clinical decision support by enabling heterogeneous hospitals to predict heart failure, stroke, and cirrhosis without sharing the raw patient data recorded in EHR. Here, the up-to-date evolving disease patterns are continually updated by the proposed model, thus supporting dynamic environments. Also, privacy-preserving gradient sharing provides early warning alerts and personalized care pathways. Likewise, the trust, traceability, and robustness against adversarial updates are ensured by the secure hospital authentication and blockchain-centric auditability. Overall, the proposed model is suitable for effective deployment in real-time distributed hospital networks, thereby enhancing the patient outcomes via a privacy-aware and continual learning CEP system.

5. CONCLUSION

This paper proposed an effective framework for FL-centric CEP and privacy preservation across distributed hospitals. In the proposed work, the number of local models was trained using different datasets, such as the heart failure prediction dataset, stroke prediction dataset, and cirrhosis prediction dataset. Then, the trained local models were updated in the global model containing multiple hospitals. Here, clinical event prediction was done using MCN-GNN, attaining an accuracy of 98.97%. Then, the model's gradients were preserved using HRLSE with a security level of 98.85%. Next, in the global model, the gradients were aggregated using CHIZD-KMC, thereby achieving an silhouette score of 0.9312. Here, the proposed HFL-based CHIZD-KMC achieved a high loss convergence rate (-0.035) and Jain's fairness index (0.95). Thereafter, the global prediction was carried out. Finally, the continual updation of the local model was done using MEPDR, attaining a retained accuracy of 98.95%. Meanwhile, all the transactions were stored in the blockchain for traceability. Hence, it was concluded that the proposed system efficiently predicted the client event, supported multi-client authentication, and preserved the gradients of EHR prediction using federated learning.

Real World Performance: By attaining high accuracy in CEP, the proposed model supports across heterogeneous hospitals without sharing raw EHR. Also, the continual learning provides continuous stability, thus making it appropriate for clinical environments. Likewise, robust

privacy protection is ensured by the encryption technique. Similarly, auditability, security, and collaboration are ensured by the hospital authentication approach. Thus, the proposed model offers scalable, secure, and reliable deployment for real-world healthcare systems.

Future Scope

In the future, the communication between the global model and local model will be optimized to ensure real-time CEP integration into the hospital information system for critical event alerts.

Dataset Link: https://www.kaggle.com/datasets/fedesoriano/heart-failure-prediction

https://www.kaggle.com/datasets/fedesoriano/stroke-prediction-dataset

https://www.kaggle.com/datasets/fedesoriano/cirrhosis-prediction-dataset

https://www.kaggle.com/datasets/iammustafatz/diabetes-prediction-dataset/data

https://www.kaggle.com/datasets/mansoordaku/ckdisease/data

Declarations

Ethics approval and consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material: The datasets generated during and/or analyzed during the current study are available from publicly available sources.

Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors Contribution: All authors have contributed equally.

Funding: No funding was received for conducting this study.

Acknowledgements: Not applicable

REFERENCES:

1. Tajabadi, M., Martin, R. & Heider, D. Privacy-preserving decentralized learning methods for biomedical applications. *Comput. Struct. Biotechnol. J.* **23**, 3281–3287; 10.1016/j.csbj.2024.08.024 (2024).

2. Haripriya, R., Khare, N., Pandey, M. & Biswas, S. A privacy-enhanced framework for collaborative Big Data analysis in healthcare using adaptive federated learning aggregation. *J. Big Data.* **12**, 1-56; 10.1186/s40537-025-01169-8 (2025).
3. Li, H. et al. Federated target trial emulation using distributed observational data for treatment effect estimation. *npj Digit. Med.* **8**, 1-15; 10.1038/s41746-025-01803-y (2025).
4. Zwiers, L. C., Grobbee, D. E., Uijl, A. & Ong, D. S. Y. Federated learning as a smart tool for research on infectious diseases. *BMC Infect. Dis.* **24**, 1-14; 10.1186/s12879-024-10230-5 (2024).
5. Ali, M., Naeem, F., Tariq, M. & Kaddoum, G. Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive survey. *IEEE J. Biomed. Health Inform.* **27**, 1-10; 10.1109/JBHI.2022.3181823 (2022).
6. Nasajpour, M. et al. Federated Learning in Smart Healthcare: A survey of applications, challenges, and future directions. *Electronics.* **14**, 1-40; 10.3390/electronics14091750 (2025).
7. Oh, W. & Nadkarni, G. N. Federated Learning in Health care Using Structured Medical Data. *Adv. Kidney Dis. Health.* **30**,1-27; 10.1053/j.akdh.2022.11.007 (2022).
8. Thakur, A. et al. Knowledge abstraction and filtering based federated learning over heterogeneous data views in healthcare. *npj Digit. Med.* **7**, 1-14; 10.1038/s41746-024-01272-9 (2024).
9. Nguyen, D. C. et al. Federated Learning for Internet of Things: A Comprehensive survey. *IEEE Commun. Surv. Tutor.* **23**, 1622–1658; 10.1109/COMST.2021.3075439 (2021).
10. Murali, L., Gopakumar, G., Viswanathan, D. M. & Nedungadi, P. Towards electronic health record-based medical knowledge graph construction, completion, and

applications: A literature study. *IEEE J. Biomed. Health Inform.* **143**, 1-13; 10.1016/j.jbi.2023.104403 (2023).

11. Javed, H., El-Sappagh, S. & Abuhmed, T. Robustness in deep learning models for medical diagnostics: security and adversarial challenges towards robust AI applications. *Artif. Intell. Rev.* **58**, 1-107; 10.1007/s10462-024-11005-9 (2025).
12. Xu, C., Qu, Y., Xiang, Y. & Gao, L. Asynchronous federated learning on heterogeneous devices: A survey. *Comput. Sci. Rev.* **50**, 1-15; 10.1016/j.cosrev.2023.100595 (2023).
13. Madathil, N. T., Dankar, F. K., Gergely, M., Belkacem, A. N. & Alrabaee, S. Revolutionizing healthcare data analytics with federated learning: A comprehensive survey of applications, systems, and future directions. *Comput. Struct. Biotechnol. J.* **28**, 1-22; 10.1016/j.csbj.2025.06.009 (2025).
14. Xue, Z. et al. A Resource-Constrained and Privacy-Preserving Edge-Computing-Enabled clinical decision system: a federated reinforcement learning approach. *IEEE Internet Things J.* **8**(11),1-17; 10.1109/JIOT.2021.3057653 (2021).
15. Zheng, Y. et al. A scoping review of self-supervised representation learning for clinical decision making using EHR categorical data. *npj Digit. Med.* **8**(1), 1-15; 10.1038/s41746-025-01692-1 (2025).
16. Meduri, K. et al. Leveraging federated learning for privacy-preserving analysis of multi-institutional electronic health records in rare disease research. *Journal of Economy and Technology* **3**, 177–189; 10.1016/j.ject.2024.11.001 (2025).
17. Messinis, S. C., Protonotarios, N. E. & Doulamis, N. Differentially private client selection and resource allocation in federated learning for medical applications using graph neural networks. *Sensors* **24**, 1–18; 10.3390/s24165142 (2024).
18. Ahmed, S., Kaiser, M. S., Chaki, S., Aloteibi, S. & Moni, M. A. Federated learning model with dynamic scoring-based client selection for diabetes diagnosis. *Knowl.-Based Syst.* **320**, 1–19; 10.1016/j.knosys.2025.113662 (2025).

19. Nagamani, G. M. & Kumar, C. K. Design of an improved graph-based model for real-time anomaly detection in healthcare using hybrid CNN-LSTM and federated learning. *Heliyon* **10**, 1–22; 10.1016/j.heliyon.2024.e41071 (2024).

20. Ali, A., Snášel, V. & Platoš, J. Health-FedNet: A privacy-preserving federated learning framework for scalable and secure healthcare analytics. *Results Eng.* **27**, 1–34; 10.1016/j.rineng.2025.106484 (2025).

21. Kuliha, M. & Verma, S. Secure internet of medical things based electronic health records scheme in trust decentralized loop federated learning consensus blockchain. *Int. J. Intell. Netw.* **5**, 161–174; 10.1016/j.ijin.2024.03.001 (2024).

22. Zhao, H., Sui, D., Wang, Y., Ma, L. & Wang, L. Privacy-Preserving Federated Learning Framework for Multi-Source Electronic Health Records Prognosis Prediction. *Sensors* **25**, 1–15; 10.3390/s25082374 (2025).

23. Abaoud, M., Almuqrin, M. A. & Khan, M. F. Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. *IEEE Access* **11**, 83562–83579; 10.1109/ACCESS.2023.3301162 (2023).

24. Akter, M., Moustafa, N. & Turnbull, B. SPEI-FL: Serverless Privacy Edge Intelligence-Enabled Federated Learning in smart Healthcare systems. *Cogn. Comput.* **16**, 2626–2641; 10.1007/s12559-024-10310-3 (2024).

25. Edelson, M., Pham, A. & Kuo, T.-T. False-positive tolerant model misconduct mitigation in distributed federated learning on electronic health record data across clinical institutions. *Sci. Rep.* **15**, 1–11; 10.1038/s41598-025-04069-2 (2025).

26. Sharma, A., Sharma, A., Sharma, A., Sharma, A. & Guo, K. Intelligent Medical Diagnosis model based on graph neural networks for medical images. *CAAI Trans. Intell. Technol.* **10**, 1201–1216; 10.1049/cit2.70020 (2025).

27. Bi, L. et al. FD-GATDR: a Federated-DeCentralized-Learning Graph Attention Network for Doctor Recommendation using EHR. *arXiv* 1–16; 10.48550/arxiv.2207.05750(2022)

28. Saemaldahr, R. & Ilyas, M. Patient-Specific Preictal Pattern-Aware Epileptic Seizure Prediction with Federated Learning. *Sensors* **23**, 1–34; 10.3390/s23146578 (2023).

29. Mao, J. et al. Toward integrating federated learning with split learning via Spatio-Temporal Graph framework for brain disease prediction. *IEEE Trans. Med. Imaging* **44**, 1–14; 10.1109/TMI.2024.3493195 (2025).

30. Lee, T.-H., Kim, S., Lee, J. & Jun, C.-H. HarmoSATE: Harmonized embedding-based self-attentive encoder to improve accuracy of privacy-preserving federated predictive analysis. *Inf. Sci.* **662**, 1–22; 10.1016/j.ins.2024.120265(2024).

31. Ali, A. A. et al. Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare. *Clin. eHealth* **8**, 125–133; 10.1016/j.ceh.2025.04.002 (2025a).

32. Tang, T. et al. Personalized Federated graph learning on Non-IID Electronic Health Records. *IEEE Trans. Neural Netw. Learn. Syst.* **35**, 1–15; 10.1109/TNNLS.2024.3370297 (2024).

33. Markkandan, S., Bhavani, N. P. G. & Nath, S. S. A privacy-preserving expert system for collaborative medical diagnosis across multiple institutions using federated learning. *Sci. Rep.* **14**, 1–23; 10.1038/s41598-024-73334-7 (2024).

34. Bhardwaj, T. & Sumangali, K. An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data. *Sci. Rep.* **15**, 1–27; 10.1038/s41598-025-04083-4 (2025).