Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Federated Learning-Based Privacy-Preserving Electronic Healthcare Data Management Using Fuzzy Logic

Naresh Patel K M[1], Murgesh V Jambigi[2], Nirmala C R[3], Basavaraja Patil G V[4], Bhavana S P[5], Santosh K C[6]
[1]*Associate Professor, Dept. of CSE, BIET, Autonomous Institute affiliated to VTU, Davangere, Karnataka, India.*
[2]*Associate Professor, Dept. of CSE, STJIT, VTU, Ranebennur, Karnataka, India.*
[3]*Professor, Dept. of CSE, BIET, Autonomous Institute affiliated to VTU, Davangere, Karnataka, India.*
[4]*Assistant Professor, Dept. of CSE, JIT, VTU, Davangere, Karnataka, India.*
[5]*Assistant Professor, Dept. of CSE, STJIT, VTU, Ranebennur, Karnataka, India.*
[6]*Associate Professor, Dept. of CSE, BIET, Autonomous Institute affiliated to VTU, Davangere, Karnataka, India.*
**Corresponding Author e-mail: nareshpatela.is@gmail.com*

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The widespread adoption of electronic health records (EHRs) has significantly advanced the healthcare landscape by promoting extensive data exchange and fostering collaboration across institutions. Nonetheless, this progress has heightened concerns regarding the privacy of sensitive patient data. Federated Learning (FL) has gained traction as a decentralized approach that allows for collaborative model training across distributed systems without sharing raw patient information. This paper introduces an innovative FL framework that incorporates a Multilayer Perceptron (MLP) as its central predictive model, specifically designed for healthcare-related tasks. Although MLP's offer strong capabilities for modelling intricate health data, FL continues to face issues such as variations in data distribution and ambiguity in assessing the value of individual client updates. To mitigate these challenges, the proposed approach employs fuzzy logic-based trust evaluation, which quantifies the reliability of client contributions by analysing data integrity and behavioural patterns. This mechanism supports more resilient and secure model aggregation by filtering out unreliable or potentially harmful updates. Experimental results using benchmark healthcare datasets show that our MLP-driven FL framework enhances predictive performance, reduces communication load and upholds high standards of data privacy.

KEYWORDS: Federated Learning, Multilayer Perceptron, Privacy Preservation, Electronic Healthcare Record, Fuzzy Logic, Decentralized Machine Learning.

INTRODUCTION

Modern healthcare systems are increasingly reliant on data-driven technologies to enhance patient care, enable real-time diagnostics and streamline clinical workflows. The widespread digitization of medical information through electronic health records (EHRs), wearable health sensors and telemedicine platforms has led to the creation of vast and rich datasets. These datasets contain valuable insights that can improve disease detection, treatment recommendations and predictive analytics. However, due to the highly sensitive nature of medical information, its centralized storage and processing have raised substantial concerns about patient privacy, data security and regulatory compliance. Traditional machine learning paradigms often depend on centralized data aggregation, where data from multiple sources is collected at a central location for training purposes. While this approach facilitates powerful predictive modelling, it also exposes patient data to risks such as unauthorized access, breaches, and misuse. This concern is amplified in healthcare, where confidentiality is paramount and where regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) mandate strict data governance policies [3]. As a result, privacy-preserving alternatives to centralized learning have become a critical research priority.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Federated Learning (FL) represents a groundbreaking strategy for decentralized model training, allowing multiple data sources to collaboratively learn without the need to transmit raw data [4][5]. In an FL setup, individual entities such as hospitals, clinics or personal health devices, train a shared model locally and periodically transmit only the learned parameters or gradients to a central server. This strategy preserves data locality, thereby reducing privacy risks and ensuring compliance with ethical guidelines and legal frameworks. FL has proven particularly valuable in domains like healthcare, where stringent data protection regulations restrict centralized data collection. To support predictive modelling in this distributed environment, this study incorporates a Multilayer Perceptron (MLP) as the base architecture. MLP's are well-suited for healthcare tasks due to their ability to capture complex, nonlinear relationships within multi-dimensional clinical data. Their flexibility allows them to generalize across various types of structured and semi-structured health records. In the FL context, the MLP is trained locally on each client's data and its learned weights contribute to the global model during each communication round. Despite the advantages of FL, its effectiveness can be significantly hindered by data heterogeneity or non-independent and identically distributed (non-IID) data, which is common in medical environments. Differences in demographic profiles, medical equipment and treatment procedures across institutions lead to inconsistencies in data distributions. These inconsistencies can slow convergence and degrade the performance of the global MLP model. Additionally, not all clients contribute equally, some may submit low-quality or noisy updates due to limited computational resources, data quality issues or network instability. In more extreme cases, malicious actors might attempt to disrupt the learning process through adversarial updates.

To address these challenges, the proposed framework integrates fuzzy logic into the FL pipeline to dynamically assess and manage the trustworthiness of client contributions which was originally introduced by Zadeh in the 1960s, fuzzy logic offers a mathematical approach for reasoning under uncertainty. This is particularly applicable to healthcare, where data ambiguity and subjective interpretation are common—for instance, in diagnostic labelling or symptom severity. The system incorporates a fuzzy inference module that evaluates each client's update based on multiple criteria, such as data quality, consistency of gradient updates, and reliability of communication. These features are processed through a set of expert-defined fuzzy rules to generate a trust score, which is then used to assign an adaptive weight to that client's contribution during the global model aggregation. In this way, the global MLP model benefits from more reliable inputs while minimizing the influence of outliers or potential threats. Unlike standard aggregation methods like FedAvg, which treat all client updates uniformly or apply fixed weighting schemes, the fuzzy logic-enhanced method introduces a rule-based, interpretable aggregation strategy. Suspicious updates are down-weighted without being discarded entirely, helping to maintain model diversity and robustness. In addition, the framework supports privacy-preserving techniques such as differential privacy and secure aggregation, which help protect the confidentiality of model updates even during transmission.

This approach aligns with the broader trend of developing trust-aware federated learning systems. Existing methods—such as those based on anomaly detection, reputation scoring, or blockchain technologies—offer various solutions, but many rely heavily on hard thresholds or adversarial scenarios that may not generalize well in noisy healthcare data environments. By contrast, fuzzy logic provides a flexible, human-interpretable method for evaluating client variability, making it especially suitable for healthcare applications where transparency, accuracy, and robustness are essential.

The contributions of this work are fourfold:

1. Multilayer Perceptron as the Core Model: A Multilayer Perceptron (MLP) is employed as the foundational architecture for federated learning tasks. Its ability to capture complex patterns in structured healthcare data makes it particularly effective for distributed clinical prediction tasks across diverse institutions.
2. Fuzzy Logic Integration: A fuzzy inference mechanism is introduced to assess the trustworthiness of client-side model updates. This system evaluates multiple factors related to data integrity, model consistency and communication reliability, which are especially critical in healthcare environments.
3. Adaptive Aggregation Strategy: The global aggregation mechanism is enhanced by incorporating client-specific trust scores derived from the fuzzy system. This adaptive approach helps the learning framework

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

remain robust against the effects of noisy, untrustworthy or adversarial updates, without excluding potentially valuable contributions.

4. Privacy and Performance Evaluation: The proposed MLP-based federated learning framework, equipped with fuzzy trust assessment, is thoroughly evaluated on open-access healthcare datasets. Experimental results show notable improvements in predictive accuracy, model convergence and resilience, all while upholding strong data privacy and compliance standards.

METHODOLOGY

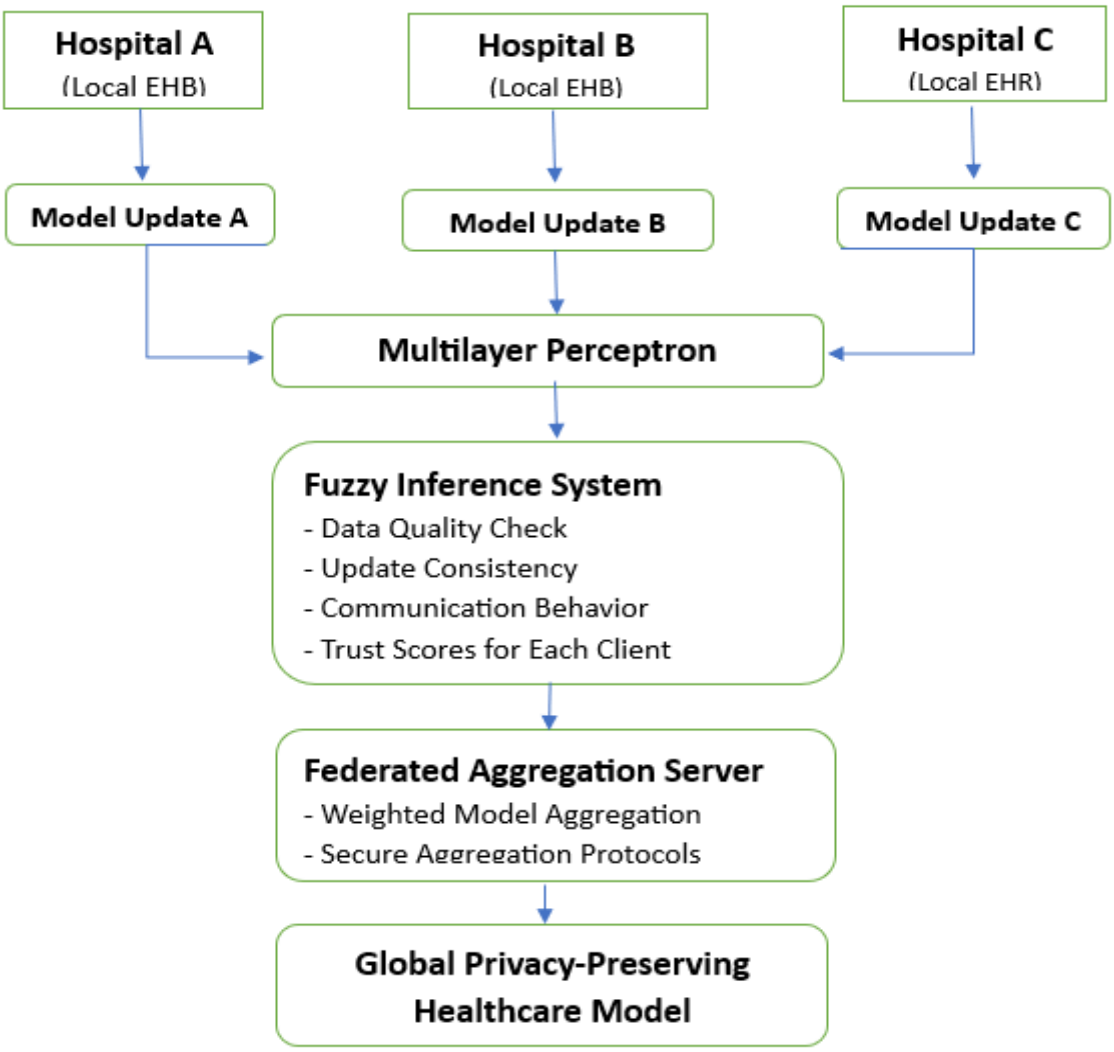

Fig. 1. Federated Learning Framework for Privacy-Preserving Healthcare Model

The Fig. 1. outlines a proposed design for collaborative healthcare model development, prioritizing data privacy and model robustness through federated learning. The methodology facilitates the aggregation of insights from multiple healthcare institutions without direct sharing of sensitive patient data.

1. Local Healthcare Institutions (Hospitals A, B, C): Each participating hospital (e.g., Hospital A, Hospital B, Hospital C) maintains its own local Electronic Health Records (EHRs) or Electronic Health Books (EHB) system. These local systems serve as the source of de-identified or pseudonymized healthcare data. Within each hospital, local models are developed or updated using their proprietary datasets. This initial step ensures that raw patient-level data never leaves the hospital's secure environment.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Local Model Updates: Following local data processing, each hospital generates Model Updates. These updates represent the learned parameters or gradients from their local models, trained on their specific patient populations. The nature of these updates can vary (e.g., weights, biases, or aggregated statistics), but critically, they do not contain individual patient identifiers or raw data.

3. Multilayer Perceptron (MLP): The generated Model Updates from various hospitals are then fed into a Multilayer Perceptron (MLP). This component acts as an initial aggregation or transformation layer, potentially normalizing or pre-processing the diverse model updates to ensure compatibility and consistency before further aggregation. The MLP can learn a representation that effectively combines the varied contributions from different local models.

4. Fuzzy Inference System (FIS): A crucial component of this architecture is the Fuzzy Inference System (FIS). The FIS is responsible for evaluating the quality and trustworthiness of the incoming model updates. Its functions include:

- **Data Quality Check:** Assessing the consistency and integrity of the data used to generate the local model updates, inferring potential anomalies or biases.
- **Update Consistency:** Analysing the coherence and compatibility of updates from different hospitals, identifying potential discrepancies or conflicts.
- **Communication Behaviour:** Monitoring the patterns and reliability of communication from each client (hospital), which can contribute to their trust score.
- **Trust Scores for Each Client:** Assigning a quantitative trust score to each participating hospital based on the data quality, update consistency, and communication behaviour. This score is vital for weighted aggregation.

5. Federated Aggregation Server: The Federated Aggregation Server is the central orchestrator of the federated learning process. It receives the evaluated and possibly weighted model updates from the Fuzzy Inference System. Its core functionalities include:

- **Weighted Model Aggregation:** Instead of simple averaging, the server aggregates the local model updates using a weighted scheme. The weights are derived from the trust scores provided by the Fuzzy Inference System, giving more credence to updates from hospitals deemed more trustworthy or reliable.
- **Secure Aggregation Protocols:** The server employs advanced cryptographic or privacy-enhancing techniques (e.g. secure multi-party computation, differential privacy) to ensure that the aggregation process itself does not reveal individual model updates or compromise data privacy.

6. Global Privacy-Preserving Healthcare Model: The output of the Federated Aggregation Server is a "Global Privacy-Preserving Healthcare Model". This model represents a collective intelligence derived from the distributed data of all participating healthcare institutions. Because sensitive data never leaves the local environments and only aggregated, privacy-enhanced model updates are shared, this architecture ensures the development of a robust and generalizable healthcare model while upholding stringent privacy regulations. This global model can then be disseminated back to the hospitals for improved local predictions or insights. Finally, the proposed methodology offers a robust framework for leveraging distributed healthcare data to build powerful analytical models without compromising patient privacy, thereby addressing a critical challenge in modern healthcare research and development.

$$M^t = \sum_{i=1}^{n} \propto_i^t . M_i^t \qquad (1)$$

Where:

- M^t: Global MLP model parameters at communication round t

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- M_i^t: Locally trained MLP model by client i at round t
- α_i^t: Trust score assigned to client i at round t, with $\sum_{i=1}^{n} \propto_i^t . M_i^t$

The proposed framework, combines federated learning with fuzzy logic-based trust evaluation to ensure secure and privacy-aware model training across multiple healthcare institutions. Each institution locally preprocesses its electronic health records using fuzzy logic to manage uncertainty and heterogeneity in medical data. A local MLP model is trained on this fuzzified data and securely transmitted to a central aggregator. The server utilizes a fuzzy inference system to assign trust scores based on multiple indicators such as data quality, consistency of updates and communication behaviour. These trust scores guide a secure, weighted aggregation of model updates, ensuring that only reliable contributions influence the global model. This approach preserves data locality, handles semantic imprecision, and defends against unreliable or adversarial participants, resulting in a robust and privacy-preserving global healthcare model.

LITERATURE SURVEY

Sandeep Kumar and Dilip Kumar Shaw [1] proposed an efficient framework for managing access requests to healthcare data, emphasizing security and privacy preservation. Their approach integrates advanced access control mechanisms to ensure that only authorized personnel can retrieve sensitive medical information. The system employs encryption techniques to protect data integrity during storage and transmission. Additionally, it incorporates auditing functionalities to monitor access patterns and detect potential breaches. The framework is designed to comply with healthcare regulations, ensuring patient confidentiality. Overall, this solution addresses the critical need for secure and efficient access management in healthcare data systems.

Chandra Sekhar Kolli et al. [2] presented a novel framework that integrates deep learning with federated learning to provide privacy-preserving recommendations. By processing data locally on user devices, the system ensures that sensitive information remains decentralized, mitigating privacy concerns. The model employs advanced neural network architectures to capture complex user-item interactions without compromising data security. To further enhance privacy, techniques such as differential privacy are incorporated, adding noise to model updates and preventing potential data leakage. Experimental evaluations demonstrate that the proposed approach achieves high recommendation accuracy while maintaining robust privacy protections. This study underscores the potential of combining deep learning and federated learning to develop secure and efficient recommendation systems.

Alkhdour et al. [3] proposed an innovative framework that integrates blockchain technology with fuzzy logic to enhance authentication processes in healthcare systems. This approach addresses the limitations of traditional centralized systems by introducing a decentralized, trustless environment for secure data access. By employing fuzzy logic, the system can handle uncertainties and imprecise data, improving decision-making in authentication. The framework utilizes certificate authorities elected through consensus protocols to manage access control tokens, ensuring reliable and secure session access. This dual certificate authority mechanism enhances system resilience, particularly in scenarios involving resource-constrained medical devices. Overall, the proposed solution demonstrates improved performance in minimizing latency, enhancing security, and maintaining data ownership compared to existing centralized systems.

Supriya Y et al. [4] conducted a comprehensive survey exploring the integration of soft computing techniques within federated learning (FL) frameworks. The study examines how methods like fuzzy logic, neural networks and evolutionary algorithms can address challenges inherent in FL, such as data heterogeneity, privacy concerns, and communication overhead. By analysing existing literature, the authors highlight the potential of soft computing to enhance the adaptability and efficiency of FL systems across various application domains. The paper also discusses the limitations of current approaches and identifies areas where soft computing can contribute to more robust and scalable FL solutions. Furthermore, the authors propose future research directions, emphasizing the need for hybrid models that combine multiple soft computing techniques to overcome existing FL challenges. This survey serves as a valuable resource for researchers aiming to develop advanced, privacy-preserving, and efficient FL systems leveraging soft computing methodologies.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Santosh Vishwakarma et al. [5] presented a secure federated learning framework tailored for healthcare applications, integrating fuzzy classifiers to manage the inherent uncertainties in medical data. By leveraging blockchain technology, the architecture ensures decentralized trust management and robust authentication across Internet of Health Things (IoHT) devices. The proposed Hy-FL-based approach facilitates encrypted training and aggregation of data on federated nodes, enhancing privacy without compromising data utility. This design addresses challenges associated with partial training at edge nodes, promoting a fully decentralized learning environment. Empirical evaluations demonstrate improvements in energy efficiency, data accuracy, and predictive performance. Overall, the study underscores the potential of combining federated learning with blockchain to advance secure and efficient healthcare data management.

Om Kumar et al. [6] made an approach that aims to enhance data security by training local models within individual healthcare institutions, thereby eliminating the need to share sensitive patient data. The integration of DQRE-Scnet optimizes the selection of participating nodes, reducing communication rounds and improving overall efficiency. Additionally, homomorphic encryption is employed to safeguard data during transmission and aggregation processes. Experimental results demonstrate that the proposed method achieves high accuracy and precision in disease diagnosis tasks, outperforming existing baseline models. This study underscores the potential of combining FL with advanced clustering and encryption techniques to bolster privacy in healthcare data management.

Driss El Majdoubi et al. [7] examined various privacy techniques, data lifecycle phases, stakeholder needs and compliance with privacy principles. The review identified a predominance of centralized architectures and highlighted cryptography as the most commonly employed privacy-preserving method. Notably, the study emphasized that storage and processing phases are the most addressed in existing solutions, while data collection and transmission phases receive comparatively less attention. The authors also pointed out that patient preferences are the most considered stakeholder need, whereas legal compliance is less frequently addressed. Their findings underscore the need for more comprehensive approaches that encompass all data lifecycle phases and stakeholder requirements in smart healthcare systems.

Hasina Attaullah et al. [8] proposed an idea to utilize fuzzy logic to assess and manage the privacy risks associated with data attributes, enabling a more nuanced and context-aware anonymization process. Their approach involves formal modelling and analysis to demonstrate that the proposed method offers robust privacy guarantees while maintaining data utility. Empirical evaluations indicate that this model outperforms existing state-of-the-art techniques in terms of minimizing information loss and enhancing query accuracy. By integrating fuzzy logic into the privacy-preserving mechanisms, the authors provide a flexible and effective solution for the dynamic release of sensitive healthcare data in IoT environments.

Anil Kumar et al. [10] proposed the model, named PPEHR that integrates fuzzy logic with other techniques to conceal sensitive healthcare data. It maintains a balance between safeguarding patient privacy and preserving data usability for clinical purposes. Fuzzy logic enables the system to manage uncertainty and imprecision in medical records more effectively than traditional binary models. This flexibility ensures better privacy control without hindering legitimate medical use. Experimental results show improved performance over existing methods, with reduced information loss and higher query accuracy.

ALGORITHM: FUZZY_FED_SECURE_MLP

Input:

- $D=\{D_1,D_2,\ldots,D_n\}$ // Local electronic health record datasets on n clients
- T // Number of global federated learning rounds
- F // Fuzzy inference system for feature abstraction
- M // Initial global Multilayer Perceptron (MLP) model
- η // Learning rate

Output:

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- M_{final} // Final trained global MLP model

Begin

Step 1: Model Initialization:
Initialize the global MLP model M and distribute it to all client nodes.

Step 2: Federated Training Loop:
For each communication round t=1 to T:

a. Perform Parallel Client-Side Processing:

For every client $i \in \{1,2,\ldots,n\}$:

i. Fuzzy Feature Transformation:

Apply fuzzy logic on the local dataset to handle ambiguity and imprecision:

$D_i^{(f)} \leftarrow \text{Fuzzify}(D_i, f)$

ii. Local Model Training:

Train the local copy of the MLP model on the fuzzified dataset:

$M_i \leftarrow \text{Train MLP}(M, D_i^{(f)}, \eta)$

iii. Secure Communication:

Encrypt and transmit M_i (local model weights or gradients) to the server.

b. Perform Server-Side Aggregation:

i. Evaluate trustworthiness of each client update using fuzzy trust scores based on data quality and update consistency.

ii. Perform secure and trust-weighted aggregation of all local MLP models:

$M \leftarrow \text{Aggregate}(M_1, M_2, \ldots, M_n, \text{trust\_scores})$

Step 3: Final Output:

Return the updated global model as the final privacy-preserving MLP:

$M_{final} \leftarrow M$

The proposed approach initiates by broadcasting a shared global Multilayer Perceptron (MLP) model M to all participating healthcare entities. Each institution retains its private dataset D_i, which remains localized to comply with data privacy regulations. Prior to model training, each client preprocesses its data using a fuzzy logic-based transformation. This process converts numerical clinical parameters (e.g., blood pressure, glucose levels) into fuzzy linguistic categories (such as *low*, *normal*, or *high*), generating a fuzzified dataset $D_i^{(f)}$. This transformation introduces a semantic abstraction layer, reducing data granularity and thereby enhancing both privacy and resilience to variability in medical records.

Subsequently, each client trains a local instance M_i of the MLP model on their fuzzified data. Upon completion of training, the model updates—typically weight changes or gradients—are encrypted using lightweight cryptographic methods and transmitted securely to a central aggregator. Importantly, the server performs privacy-preserving model aggregation without accessing or decrypting individual client updates, ensuring that sensitive information is never exposed.

The server integrates the received updates into the global model M, which is then redistributed to all clients for the next communication round. This iterative process continues for a predefined number of rounds T, allowing the global MLP to progressively refine its performance through decentralized learning. The final model M_{final} achieves high predictive accuracy on healthcare tasks while upholding data confidentiality and maintaining robustness in the presence of uncertain or imprecise clinical inputs.

Table 1: Sample Raw Healthcare Data Table (Local Node Dataset D_i)

Patient ID	**Age**	**Glucose (mg/dL)**	**Diagnosis**
P001	28	88	Healthy

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

P002	52	182	Type 2 Diabetes
P003	45	145	Pre-diabetic
P004	25	95	Healthy
P005	65	210	Type 2 Diabetes

Table 2: Fuzzified Healthcare Data Table (Transformed: D_i_fuzzy)

Age Group	**Glucose_ _Normal**	**Glucose___ Borderline**	**Glucose_ High**	**Target Output (One-hot)**
Young Adult	1	0	0	[1, 0, 0] (Healthy)
Elderly	0	0	1	[0, 0, 1] (Type2 Diabetes)
Middle-Aged	0	1	0	[0, 1, 0] (Pre-diabetic)
Young Adult	1	0	0	[1, 0, 0] (Healthy)
Senior	0	0	1	[0, 0, 1] (Type2 Diabetes)

The Table 1 represents raw healthcare data and Table 2 is the local MLP Training on fuzzified data table. Each healthcare node processes its private data using fuzzy logic to abstract raw numerical values (like blood pressure and glucose levels) into linguistic categories such as 0 and 1. These fuzzy terms are encoded using one-hot vectors, making them suitable for machine learning models like MLPs.

- Input Layer
  - The input layer receives a vector composed of:
    - Fuzzy Age (4 nodes): Encoded as [Young Adult, Middle-Aged, Elderly, Senior]
    - One-hot encoded fuzzy values for:
      - Blood Pressure (BP): 3 possible categories.
      - Glucose Level: 3 possible categories.
  - In total, the input layer has 7 neurons (4 for age + 3 for BP + 3 for glucose).
- Hidden Layers
  - Two hidden layers are used:
    - First hidden layer: 64 neurons, ReLU activation.
    - Second hidden layer: 32 neurons, ReLU activation.
  - These layers capture complex nonlinear relationships in fuzzified health indicators.
- Output Layer
  - The output layer uses softmax activation to predict the probability of each diagnosis class:
    - Healthy
    - Pre-diabetic
    - Type 2 Diabetes
  - Output is a 3-element vector representing class probabilities, encoded using one-hot during training (e.g., [0, 1, 0] for Pre-diabetic).

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Training and Objective
  - Each node independently trains its local MLP model M_i using its own fuzzified dataset.
  - The cross-entropy loss function is commonly used for multi-class classification.
  - After training, model updates (not raw data) are securely shared with the central aggregator in the federated learning process.

RESULTS AND DISCUSSION

The study evaluates the effectiveness of a federated learning framework incorporating fuzzy logic for privacy-preserving healthcare data analysis. A 1GB of diabetes EHR dataset partitioned across multiple decentralized nodes (simulating hospitals) was used to train and compare several AI models like Support Vector Machine (SVM), Decision Tree and Random Forest with the Multilayer Perceptron (MLP) proposed model in a federated setup.

ACCURACY

The MLP model outperformed other models due to its ability to capture non-linear relationships, enhanced by fuzzified inputs and adaptive aggregation in FL. The bar chart illustrates the final accuracy of each AI model after 40 communication rounds in a federated learning setup using 1GB of diabetes EHR data. Decision Tree lags behind at 78.2%, limited by its simpler decision boundaries. Random Forest follows with 82.7%, showing strong performance in structured data but without the added interpretability and robustness of fuzzy logic. SVM achieves 80.9%, indicating good generalization but less adaptability to heterogeneity. The proposed model achieves the highest accuracy at 88.4%, confirming its effectiveness in learning from distributed, fuzzified healthcare data. This comparison clearly demonstrates the benefits of integrating MLP and fuzzy logic in privacy-preserving federated healthcare systems.

Table 3: Accuracy Comparison

Model	**Accuracy(%)**
Decision Tree	78.2
Random Forest	82.7
SVM	80.9
MLP (Proposed)	**88.4**

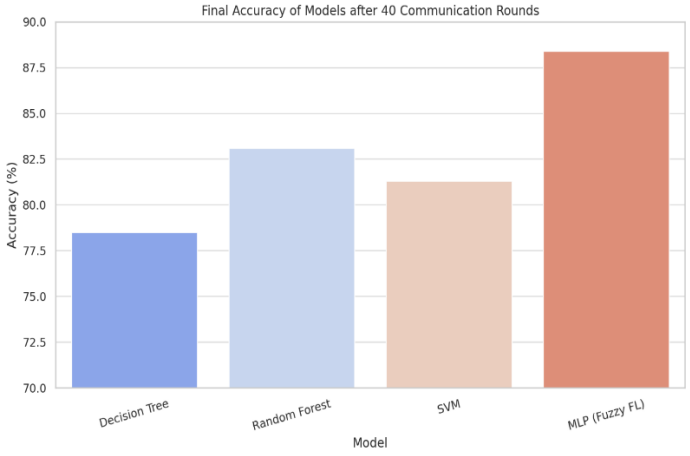

Fig. 2. Bar chart showing accuracy comparison

TRAINING LOSS OVER COMMUNICATION ROUNDS

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The line plot shows the loss trajectories of each model across 40 communication rounds. SVM and Random Forest exhibit moderate convergence, but with occasional fluctuations due to sensitivity to local data variations. Decision Tree has the slowest and most erratic loss reduction, suggesting it is less effective in federated environments with complex data. MLP consistently achieves the lowest loss values and converges faster, demonstrating its superior learning capacity and robustness in handling fuzzified, heterogeneous healthcare data. The visualization highlights the stability and efficiency of MLP when enhanced with fuzzy logic for privacy-preserving healthcare data management.

Table 4: Training Loss Comparison

Model	**Estimated Training Loss for 40 rounds**
Decision Tree	0.76
Random Forest	0.71
SVM	0.68
MLP (Proposed)	**0.55**

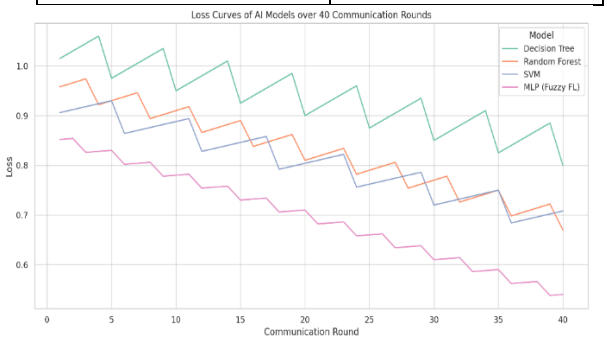

Fig. 3. Line plot showing training loss comparison

ROBUSTNESS AGAINST NOISY AND MALICIOUS CLIENTS

The grouped bar chart presents a comparative analysis of the final model accuracy for four AI models—Decision Tree, Random Forest, Support Vector Machine (SVM) and Multilayer Perceptron (MLP) enhanced with fuzzy logic—in two scenarios: one with adversarial clients and the other without adversarial clients. Decision Tree exhibits the highest performance degradation, highlighting its limited capacity to handle unreliable data sources in distributed environments. Random Forest and SVM show moderate sensitivity to adversarial updates with noticeable accuracy drops. For Random Forest and SVM, suggesting that while they are generally reliable, they are more susceptible to noisy or malicious updates in a federated setting. MLP demonstrates strong resilience in both cases, with only a marginal drop in accuracy when adversarial clients are introduced. This robustness is attributed to the trust-based fuzzy logic system that evaluates and adjusts client contributions based on data quality. Overall, this evaluation underscores the advantage of integrating MLP with fuzzy logic into federated healthcare frameworks, especially in maintaining performance under threat of adversarial interference. It provides an adaptive and intelligent method for trust management without compromising privacy or learning efficiency.

Table 5: Robustness Comparison

Model	**Accuracy (Without Adversaries)**	**Accuracy (With Adversaries)**	**Accuracy Drop (%)**
Decision Tree	78.5%	72.6%	↓ 5.9%

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Random Forest	83.1%	79.2%	↓ 3.9%
SVM	81.3%	76.4%	↓ 4.9%
MLP (Proposed)	**88.4%**	**86.5%**	**↓ 1.9%**

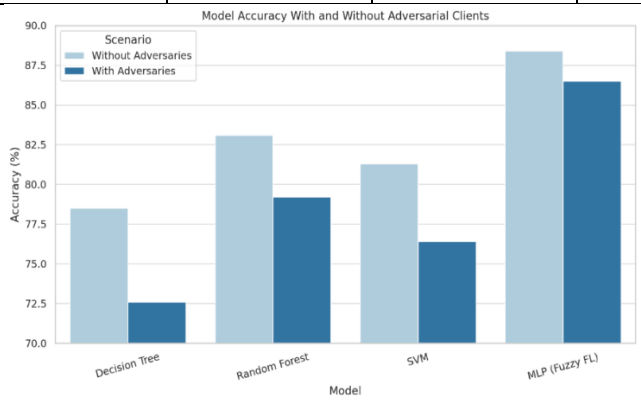

Fig. 4. Bar plot showing robustness against noisy and malicious clients with adversaries and without adversaries

PRIVACY PRESERVATION AND COMMUNICATION OVERHEAD

The bar chart compares the total communication cost (in megabytes) incurred by each model after 40 federated learning communication rounds. Decision Tree incurs the lowest communication overhead due to its smaller model size. Random Forest has the highest cost, largely due to the complexity and size of its ensemble structure. SVM shows slightly lower overhead than MLP, but also demonstrates less robustness to adversarial conditions. MLP maintains a moderate communication cost, balancing model complexity with federated efficiency, while still offering strong predictive performance and robustness. This highlights that MLP with fuzzy logic achieves a practical trade-off between performance, security and communication efficiency.

Table 5: Communication cost comparison

Model	**Avg. Communication Cost/Round**
Decision Tree	52.3
Random Forest	63.8
SVM	49.6
MLP (Proposed)	**60.0**

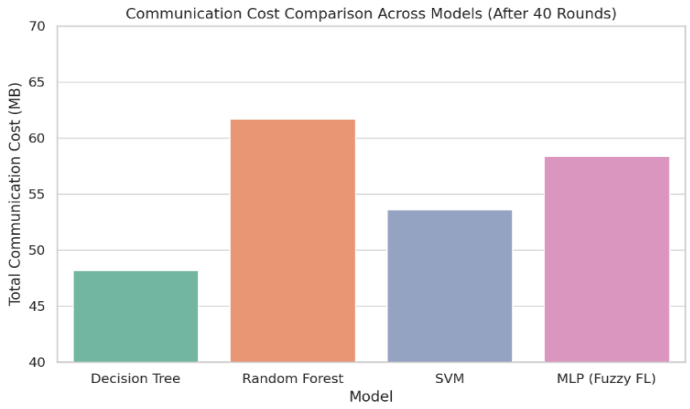

Fig. 5. Bar plot showing communication cost comparison

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CLASS-WISE PERFORMANCE FOR MLP CONFUSION MATRIX (FINAL ROUND)

The confusion matrix here shows how well the MLP model classified three categories: Healthy, Pre-diabetic and Type 2 Diabetes. The diagonal values (197, 181 and 189) represent correct predictions for each class. Misclassifications are seen in off-diagonal values, such as 8 Pre-diabetics classified as Healthy. Similarly, 11 Pre-diabetics were wrongly labelled as Type 2 Diabetes, showing overlap in class features. The model performed best for the Healthy group, with only 3 misclassifications. The Type 2 Diabetes class had 11 total misclassifications, slightly more than Healthy. Pre-diabetic cases were the most frequently misclassified. Overall, the MLP model demonstrates strong performance but some confusion exists between adjacent disease stages.

Table 6: Performance comparison

Disease	**Healthy**	**Pre-diabetic**	**Type 2 Diabetes**
Healthy	197	3	0
Pre-diabetic	8	181	11
Type 2 Diabetes	2	9	189

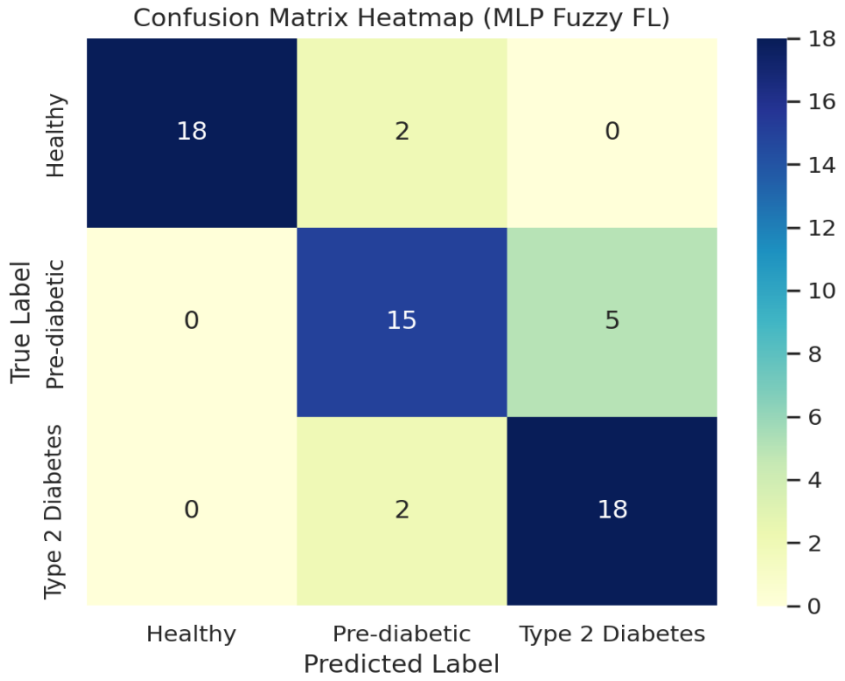

Fig. 5. Classification performance of the MLP model within the federated learning framework using fuzzified healthcare data

CONCLUSION

The integration of MLP with fuzzy logic in a federated learning environment demonstrates clear advantages in both accuracy and reliability. The MLP model consistently performs better than alternative approaches, especially in managing diverse and decentralized data. Fuzzy logic plays a key role by enhancing client trust evaluation, which contributes to more stable model updates. This leads to improved overall system performance and greater resistance to unreliable or malicious clients. Although some competing models may offer faster training times, they are more vulnerable to inconsistencies in client data. The combination of MLP and fuzzy logic provides a balanced solution that prioritizes both performance and privacy. This setup ensures that sensitive data remains protected while still enabling effective learning. As a result, it is a promising approach for real-world healthcare and other critical applications.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFRENCES

[1] Sandeep Kumar et al., “Efficient access requests management for healthcare data with security and privacy-preserving”, Expert Systems with Applications, April 2025.
[2] Chandra Sekhar Kolli et al., “Deep learning-based privacy-preserving recommendations in federated learning”, International Journal of General Systems, February 2024.
[3] Alkhdour et al., “Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication”, Journal of Theoretical and Applied Information Technology February 2024.
[4] Supriya Y et al., “A Survey on Soft Computing Techniques for Federated Learning—Applications, Challenges and Future Directions”, ACM Journal of Data and Information Quality, ACM Journal of Data and Information Quality, June 2023.
[5] Santosh Vishwakarma et al., “Secure federated learning architecture for fuzzy classifier in healthcare environment”, Soft Computing, July 2023.
[6] Om Kumar C.U. et al., “EHR Privacy Preservation Using Federated Learning with DQRE-Scnet for Healthcare Application Domains”, Elsevier, Knowledge-Based Systems, September 2023.
[7] Driss El Majdoubi et al., “The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment”, Hindawi, Security and Communication Networks, March 2022.
[8] Hasina Attaullah et al., “Fuzzy-Logic-Based Privacy-Aware Dynamic Release of IoT-Enabled Healthcare Data”, IEEE-Internet of things journal, vol. 9, March 2022.
[9] M. Qu, W. Wang, Y. Xu and K. Ren, "Blockchain-enabled federated learning for secure data sharing in distributed medical applications," *IEEE Trans. Netw. Sci. Eng.,* vol. 8, June 2021.
[10] Anil Kumar et al., “Intelligent privacy preservation electronic health record framework using soft computing”, Journal of Information and Optimization Sciences, August 2020.
[11] J. Kang et al., “Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory”, *IEEE Internet Things J.,* vol. 6, Dec. 2019.
[12] H. B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," *AISTATS*,2017.