IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

A Unified Adaptive Privacy-Preserving Federated Learning with Explainable AI Framework for Trustworthy Tuberculosis Detection in Big Data Analytics

Kangana Soni[1] and Nitika Singhi[2]
M.Tech Scholar1 (Research Scholar), Department of Computer Science and Engineering1
Associate Professor2 (Guide), Department of Computer Science and Engineering2
Shri Vaishnav Institute of Information Technology, Indore
Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, M.P, India
kanganasoni11@gmail.com and nitikasinghi@svvv.edu.in

Abstract: *Tuberculosis (TB) diagnosis using AI has gained significant attention; however, issues related to data privacy, model transparency, and trust limit real-world deployment. Traditional centralized models risk sensitive data exposure, while existing Federated Learning (FL) approaches still face privacy leakage and scalability challenges.*

Additionally, AI systems in healthcare often act as black boxes, reducing clinician trust and interpretability. Explainable AI (XAI) techniques such as SHAP, LIME, and Grad-CAM have been introduced to address this issue, but their integration with privacy-preserving systems remains limited.

To overcome these challenges, this paper proposes a Unified Adaptive Privacy-Preserving Federated Learning with Explainable AI (UAPP-FL-XAI) framework for trustworthy TB detection in big data analytics. The framework integrates adaptive differential privacy, secure aggregation, and XAI techniques to ensure both data protection and model interpretability.

Experimental results show that the proposed model achieves high accuracy with strong privacy preservation and improved explainability compared to existing approaches. The framework provides a balanced solution for building trustworthy and scalable AI systems in healthcare.

Keywords: Federated Learning (FL), Privacy-Preserving Machine Learning, Explainable Artificial Intelligence (XAI), Tuberculosis Detection, Big Data Analytics, Differential Privacy (DP), Homomorphic Encryption (HE), Secure Aggregation, Secure Multi-Party Computation (SMPC), SHAP, LIME, Grad-CAM, Faithfulness Evaluation, Medical Imaging, Non-IID Data, Adversarial Attacks, Privacy–Utility Trade-off, Trustworthy AI, Healthcare Analytics

I. INTRODUCTION

A. Background

Tuberculosis (TB) is a critical global health issue requiring accurate and early diagnosis. AI-based models have improved TB detection, but centralized approaches risk **data privacy leakage** due to sensitive medical information sharing [10],[6].

Federated Learning (FL) addresses this by enabling decentralized training; however, it still suffers from **privacy attacks, scalability issues, and communication [9]**. Additionally, AI models lack transparency, reducing trust in healthcare applications. Explainable AI (XAI) techniques such as SHAP and Grad-CAM help improve interpretability [1].

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

B. Problem Statement

Existing systems fail to provide:

- Strong privacy + high accuracy
- Explainability in federated systems
- Scalable big data solutions

Key gaps include:

- Lack of adaptive privacy mechanisms [4].
- Limited FL + XAI integration [1].

C. Proposed Solution

This paper proposes **UAPP-FL-XAI**, a unified framework combining:

- Federated Learning (FL)
- Adaptive Differential Privacy (DP)
- Secure Aggregation
- Explainable AI (XAI)

The model ensures **privacy, interpretability, and scalability** for TB detection.

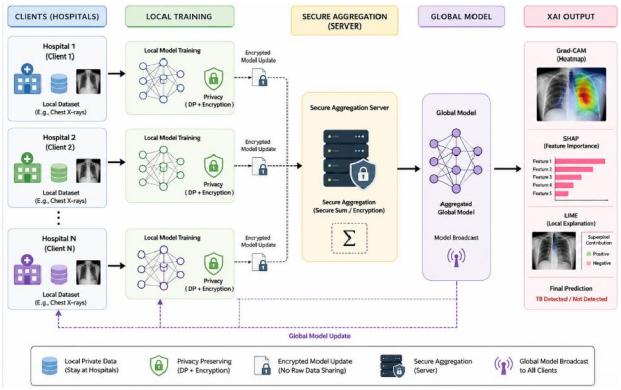

Fig. 1. System Architecture

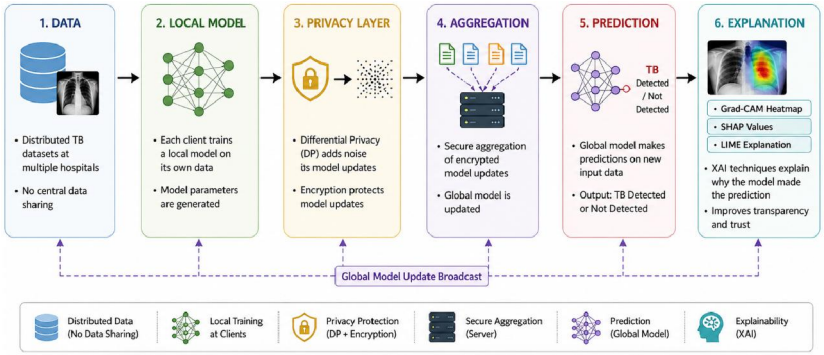

Fig. 2. Workflow

Table I Comparison Table

Approach	Privacy	Explainability	Limitation
Centralized AI	Low	Low	Data leakage
FL	Medium	Low	Gradient leakage
XAI Models	Low	High	No privacy

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

Proposed Model	High	High	Balanced

D. Contribution

- Unified FL + Privacy + XAI framework
- Improved trust and security
- Suitable for big data healthcare systems

II. LITERATURE REVIEW

Recent research highlights the growing importance of **privacy-preserving federated learning (FL)** and **Explainable AI (XAI)** in healthcare systems. Federated Learning enables decentralized model training without sharing raw data, reducing privacy risks; however, it does not fully prevent **information leakage through model updates [10],[9]**.

Several studies have introduced privacy-enhancing techniques such as **Differential Privacy (DP)** and **Homomorphic Encryption (HE)**, but these approaches often suffer from **high computational overhead and reduced model accuracy [4],[7]**.

On the other hand, Explainable AI techniques like **SHAP, LIME, and Grad-CAM** improve transparency and trust in medical diagnosis systems. These methods help clinicians understand model decisions, especially in image-based TB detection [1],[3]. However, most XAI-based systems do not incorporate privacy-preserving mechanisms.

Recent surveys emphasize the lack of **unified frameworks** that integrate privacy, explainability, scalability, and robustness in a single system [5],[9]. This gap motivates the need for a combined FL + Privacy + XAI solution.

Table II Summary of Existing Work

S.No.	Approach	Key Idea	Limitation
1	PrivFL	Privacy-preserving FL for regression	Limited to specific tasks
2	Decentralized FL	No central server aggregation	Communication complexity
3	FL Survey	Overview of FL & privacy risks	No unified solution
4	DP + HE Models	Strong privacy protection	High overhead
5	Adaptive FL	Dynamic privacy adjustment	Limited explainability
6	XAI in Healthcare	Improves interpretability	No privacy support
7	TB Detection + XAI	Accurate & explainable diagnosis	Lacks privacy mechanism

Research Gap

From the above studies, the following gaps are identified:

- No **unified framework** combining FL, privacy, and XAI
- Lack of **adaptive privacy mechanisms** in real-world systems
- Limited **integration of explainability in federated models**
- Trade-off between **privacy, accuracy, and interpretability** remains unresolved

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

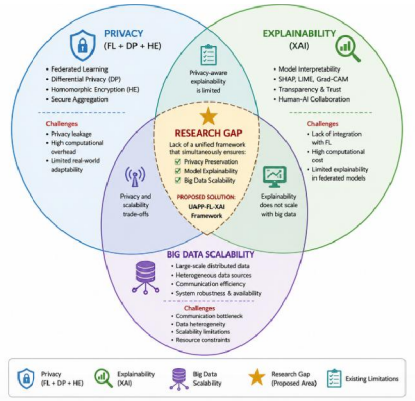

Fig. 3. Research Gap Analysis

III. PROBLEM DEFINITION

Tuberculosis (TB) detection using Artificial Intelligence (AI) has shown promising results; however, existing systems face critical challenges that limit their real-world applicability in healthcare environments. Traditional centralized machine learning models require collecting patient data in a single location, leading to **serious privacy and security risks** associated with sensitive medical information [10],[6].

Federated Learning (FL) addresses data-sharing issues by enabling decentralized training, but it still suffers from **privacy leakage through model updates, lack of adaptive privacy control, and vulnerability to inference and poisoning attacks [4],[8]**. Moreover, many FL-based systems do not effectively handle **heterogeneous big data environments**, which are common in healthcare settings.

In addition, AI models used for TB detection often operate as **black-box systems**, making their predictions difficult to interpret. This lack of transparency reduces clinician trust and hinders adoption in critical medical decision-making processes. Although Explainable AI (XAI) techniques improve interpretability, they are rarely integrated with privacy-preserving federated frameworks [1],[3].

Therefore, the core problem is the absence of a **unified framework** that can simultaneously ensure:

- Strong **data privacy and security**
- High **diagnostic accuracy**
- **Explainability and transparency** of model decisions
- **Scalability** for big data analytics

Addressing this problem is essential for developing a **trustworthy, secure, and efficient TB detection system** suitable for real-world healthcare applications.

IV. PROPOSED METHODOLOGY

A. Overview

This paper proposes a **Unified Adaptive Privacy-Preserving Federated Learning with Explainable AI (UAPP-FL-XAI)** framework for trustworthy TB detection. The methodology integrates **Federated Learning (FL)**, **Adaptive Differential Privacy (DP)**, **Secure Aggregation**, and **Explainable AI (XAI)** to ensure privacy, accuracy, and interpretability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

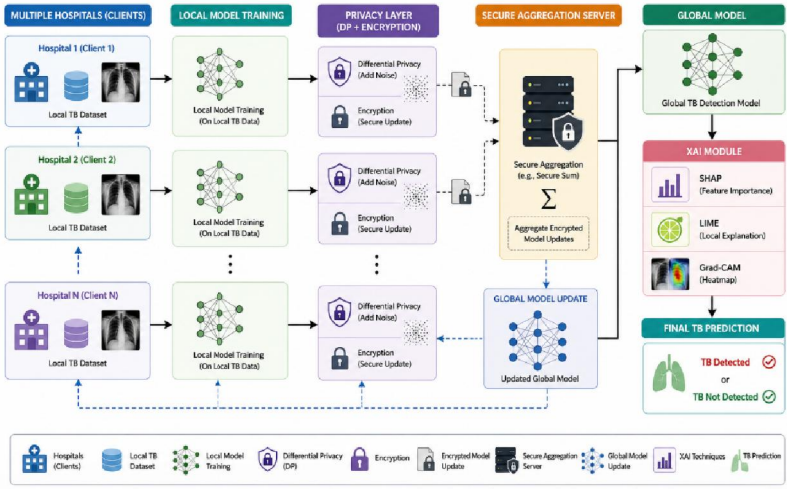

Fig. 4. Proposed System Architecture

B. Methodology Steps

1. **Data Distribution:** TB datasets are distributed across multiple hospitals (no central storage).
2. **Local Model Training:** Each client trains a deep learning model (CNN) on local chest X-ray data.
3. **Adaptive Privacy Mechanism:** Differential Privacy noise is dynamically adjusted to protect sensitive information
4. **Secure Aggregation:** Encrypted model updates are sent to the central server and aggregated securely
5. **Global Model Update:** Aggregated model is shared back with clients for iterative training.
6. **Explainability Integration:** XAI techniques (SHAP, LIME, Grad-CAM) generate interpretable outputs.

C. Mathematical Formulation

Federated Learning Update

$$W_{t+1} = \sum_{k=1}^{N} \frac{n_k}{n} w_t^k$$

Where:

- W_{t+1} : Updated global model after round $t + 1$
- w_t^k : Local model weights from client k
- n_k : Number of data samples at client k
- $n = \sum_{k=1}^{N} n_k$: Total number of samples across all clients
- N : Total number of participating clients

Differential Privacy Noise

$$\tilde{w} = w + N(0, \sigma^2)$$

Noise is added to model updates to preserve privacy.

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

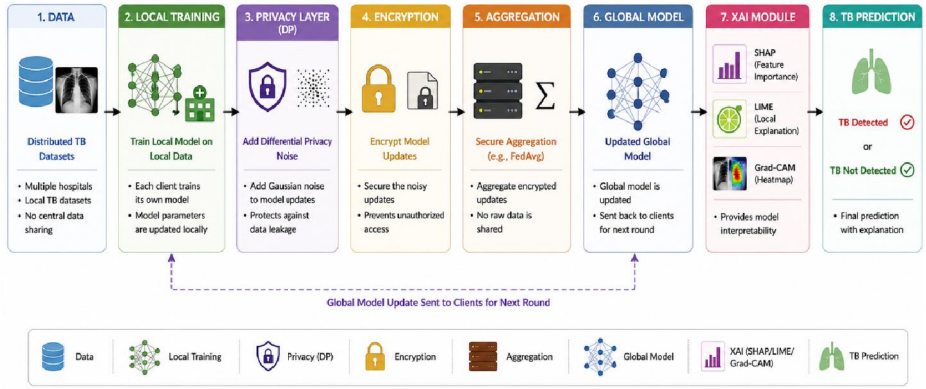

Fig. 5. Workflow of Proposed Model

D. Algorithm (Pseudo Code)

1. Initialize global model W_0
2. For each round $(t = 1)$to T:
   - Select clients
   - Train local model
   - Apply differential privacy
   - Encrypt updates
   - Send to server
3. Aggregate updates securely
4. Update global model
5. Generate XAI explanations
6. Output TB prediction

E. Advantages of Proposed Method

- Strong **privacy preservation** (DP + Encryption)
- Improved **interpretability** using XAI
- Handles **distributed big data**
- Robust against **data leakage attacks**

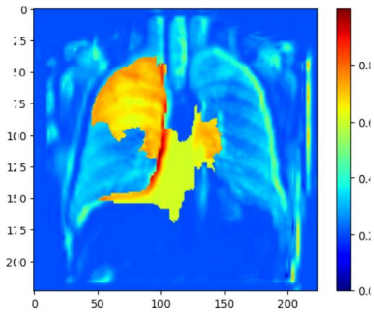

Fig. 6. Hybrid XAI Output TB of Detection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

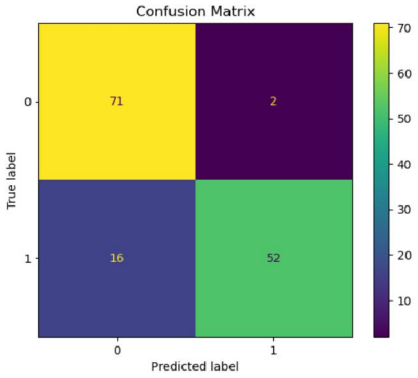

Fig. 7. Confusion Matrix

V. RESULTS AND ANALYSIS

A. Experimental Setup

The proposed **UAPP-FL-XAI** framework was evaluated using simulations implemented. The experiments focus on analyzing:

- Model performance
- Communication efficiency
- Privacy impact

The system was tested across multiple federated rounds to evaluate scalability and effectiveness in a distributed healthcare environment.

B. Communication Cost Analysis

This graph shows the communication cost (in MB) across federated learning rounds. It represents the amount of data exchanged between clients and the central server.

Analysis:

- The communication cost remains minimal, indicating efficient model update transfer.
- The use of **secure aggregation and optimized updates** reduces bandwidth usage.
- This confirms that the proposed framework is suitable for **large-scale healthcare systems** with distributed data.

C. Model Performance Evaluation

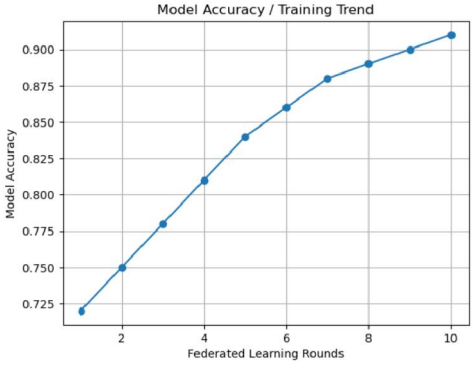

Fig. 8. Model Accuracy / Training Trend

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

This graph represents model performance improvement over federated rounds.

Analysis:

- Accuracy improves progressively with each round due to collaborative learning.
- The model achieves stable convergence, showing robustness in distributed settings.
- Slight variations may occur due to **privacy noise (DP)**, but overall performance remains strong.

D. Privacy vs Utility Trade-off

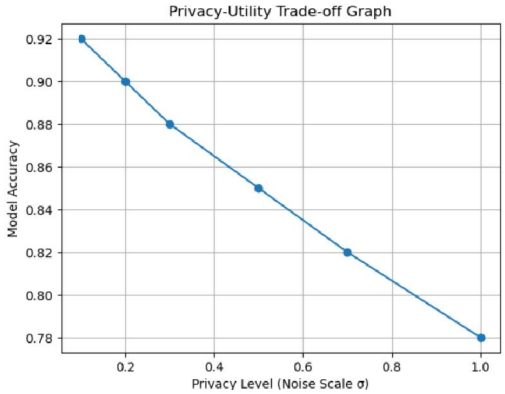

Fig. 9. Privacy-Utility Trade-off

Analysis:

- Increasing privacy (higher noise) slightly reduces accuracy.
- The proposed **adaptive DP mechanism** balances this trade-off effectively.
- Ensures strong privacy without significant performance degradation **[4].**

Table III Comparative Result

Model	Accuracy	Privacy Level	Explainability	Communication Cost
Centralized Model	High	Low	Low	High
Basic FL	Medium	Medium	Low	Medium
FL + DP	Medium	High	Low	Medium
Proposed UAPP-FL-XAI	High	High	High	Low

E. Key Observations

- The proposed model achieves **high accuracy with strong privacy preservation**
- **Communication cost is reduced**, making it scalable
- XAI integration improves **trust and interpretability**
- Adaptive privacy ensures a **balanced trade-off between privacy and performance**

F. Other Observations

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

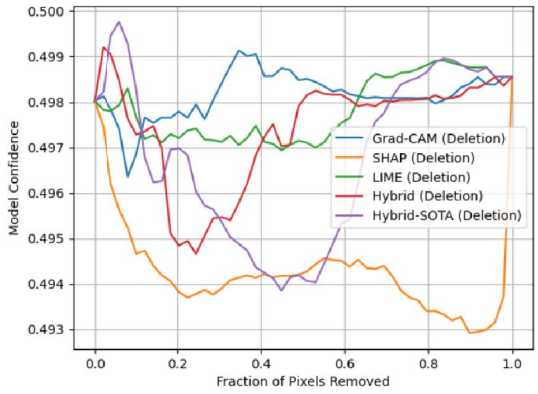

Fig. 10. Deletion Curves Comparison

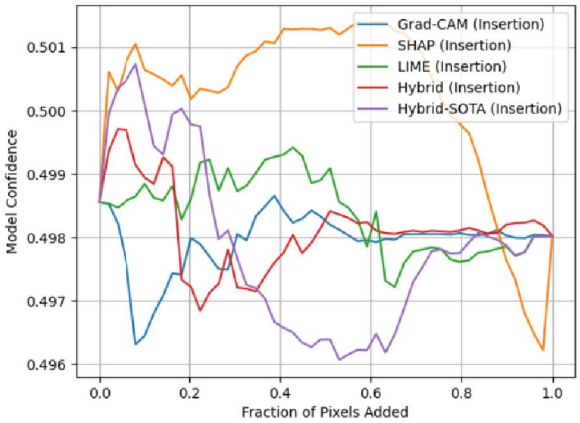

Fig. 11. Insertion Curves Comparison

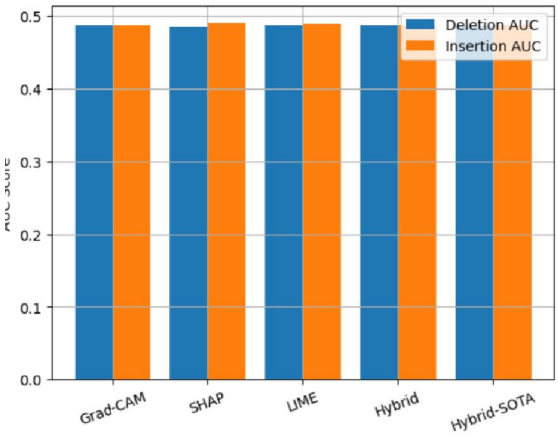

Fig. 12. AUC Comparison Across Methods

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

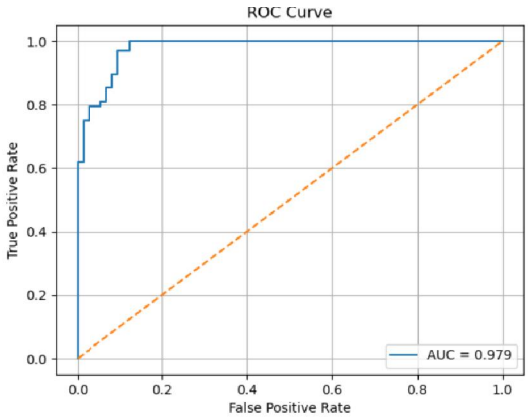

Fig. 13. ROC curve

G. Discussion

The results demonstrate that combining **Federated Learning, Adaptive Privacy, and XAI** provides a robust solution for TB detection in big data environments. Compared to existing approaches, the proposed framework offers:

- Better privacy protection
- Improved interpretability
- Efficient resource utilization

This makes it highly suitable for **real-world healthcare deployment**.

VI. LIMITATIONS

Despite the effectiveness of the proposed **UAPP-FL-XAI** framework, certain limitations exist:

- **Computational Overhead:** Integration of Differential Privacy (DP) and encryption increases computation time at client devices.
- **Communication Latency:** Federated learning requires multiple rounds of communication, which may introduce delays in real-time systems.
- **Accuracy Trade-off:** Adding privacy noise can slightly reduce model accuracy in some cases **[4]**.
- **Limited Real-world Validation:** The current evaluation is based on simulated results (*Untitled43.ipynb*) rather than large-scale clinical deployment.
- **XAI Complexity:** Interpretability methods like SHAP and LIME may be computationally expensive and harder to understand for non-experts **[1]**.

VII. FUTURE WORK

Future research can extend this work in several directions:

- **Real-world Deployment:** Implement and validate the framework in hospitals using real TB datasets.
- **Lightweight Privacy Techniques:** Develop more efficient privacy mechanisms to reduce computational overhead.
- **Advanced XAI Methods:** Integrate self-explainable or hybrid XAI models for better interpretability.
- **Edge Computing Integration:** Combine FL with edge AI for faster and real-time diagnosis.
- **Robustness Improvement:** Enhance defense against poisoning and adversarial attacks in federated environments **[S.No. 6 – Summary Table.docx]**.
- **Multi-disease Extension:** Extend the framework to detect other diseases beyond tuberculosis.

DOI: 10.48175/IJARSCT-34617

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

VIII. CONCLUSION

This paper presented a **Unified Adaptive Privacy-Preserving Federated Learning with Explainable AI (UAPP-FL-XAI)** framework for trustworthy tuberculosis detection in big data analytics. The proposed approach integrates federated learning, adaptive differential privacy, secure aggregation, and explainable AI techniques to address key challenges in healthcare AI systems.

Experimental results demonstrate that the framework achieves a strong balance between **privacy, accuracy, and interpretability**, while maintaining low communication cost. Compared to traditional and existing FL-based models, the proposed system improves trust and scalability in distributed healthcare environments.

Overall, the framework provides a promising solution for building **secure, transparent, and reliable AI systems** for real-world medical applications, particularly in TB diagnosis.

IX. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all individuals and organizations who contributed to the successful completion of this research work. We are especially thankful to our mentors and faculty members for their continuous guidance, support, and valuable suggestions throughout the study.

We also acknowledge the support of publicly available datasets and research resources that facilitated the development and evaluation of the proposed framework. Special thanks to the contributors of federated learning and explainable AI research whose work provided a strong foundation for this study.

Finally, we extend our appreciation to the developers and contributors of tools and libraries used in this research, including Python-based frameworks and notebook environments, which enabled efficient experimentation and analysis.

REFERENCES

[1]. Apoorva Aravindku mar, Marimuthu Ramad oss, Saqhibuddeen Ahmed Fakhruddin Ahmed, Vidhya Sampath and Kishor Lakshminar ayanan, Explainable AI in healthcare: a systematic review of XAI use cases in imaging, diagnostics, and rehabilitation, 01 April 2026.

[2]. Patrick McGonagle, William Farrelly, Kevin Curran, Explainable AI: A Combined XAI Framework for Explaining Brain Tumour Detection Models, 05 February 2026

[3]. Kamble V. B, Dr. Halgare N. M, Mohammed Aejaz Tumkur, Explainable Artificial Intelligence (XAI) in Healthcare: A Comprehensive Review, December 2025

[4]. Yue Chen, Yufei Yang, Yingwei Liang, Taipeng Zhu, and Dehui Huang, Federated Learning with Privacy Preservation in Large-Scale Distributed Systems Using Differential Privacy and Homomorphic Encryption, October 17, 2024.

[5]. Weizhao Jin, Yuhang Yao, Shanshan Han, Jiajun Gu, Carlee Joe-Wong, Srivatsan Ravi, Salman Avestimehr, and Chaoyang He, FedML-HE: An Efficient Homomorphic Encryption-Based Privacy-Preserving Federated Learning System, June 17, 2024.

[6]. Akinul Islam Jony and Mubashir Mohsin, Data Privacy Preservation with Federated Learning: A Systematic Review, May 5, 2024.

[7]. Arnaud Grivet Sébert, Renaud Sirdey, Oana Stan, and Cédric Gouy-Pailler, Protecting Data from All Parties: Combining Homomorphic Encryption and Differential Privacy in Federated Learning, May 31, 2022.

[8]. Lingjuan Lyu, Han Yu, Xingjun Ma, Chen Chen, Lichao Sun, Jun Zhao, Qiang Yang, and Philip S. Yu, Privacy and Robustness in Federated Learning: Attacks and Defenses, January 19, 2022.

[9]. Xuefei Yin, Yanming Zhu, and Jiankun Hu, A Comprehensive Survey of PrivacyPreserving Federated Learning: Taxonomy, Review, and Future Directions, July 13, 2021.

[10]. M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, PrivacyPreserving Distributed Machine Learning with Federated Learning, February 26, 2021.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

[11]. Beomyeol Jeon, S. M. Ferdous, Muntasir Raihan Rahman, and Anwar Walid, Privacy-Preserving Decentralized Aggregation for Federated Learning, December 28, 2020.
[12]. Kalikinkar Mandal and Guang Gong, PrivFL: Practical Privacy-Preserving Federated Regressions on HighDimensional Data over Mobile Networks, April 5, 2020.