FL-DRNA: Federated Learning with Decentralized Record Network based Auditing

Dr. Suman Jayakumar[1], Dr. Shashi Kant Gupta[2]
[1] Post-Doctoral Research Scholar, Lincoln University College, Malaysia
[2] Adjunct Professor, Lincoln University College, Malaysia
Email ID: pdf.suman@lincoln.edu.my, shashigupta@lincoln.edu.my

---

Abstract: The proliferated utilization of Artificial Intelligence (AI) has been emerging high in healthcare sector which has introduced potential benefits in various form while it has induced critical security challenges at same time. Specifically, the problem of data privacy is on risk for multi-chains hospital or any healthcare units whose data is maintained in distributed system. Therefore, this paper presents an innovative framework known as Federated Learning with Decentralized Record Network based Auditing (FL-DRNA) which is meant for addressing this problem of data privacy without sharing any form of sensitive information of patient. A collaborative model training is facilitated by proposed model connecting multiple healthcare units while Advanced Encryption Standard (AES) is used for preserving the privacy during communication as well as during validating the transactions. The model unifies decentralized auditing with adaptive federated aggregation for improving communication integrity, trust validation, and transparency. Adopting standard benchmarked MIMIC-III dataset, the outcome of the FL-DRNA is noted to be significantly better in contrast to existing standard approaches. FL-DRNA reports of contributing to 97.42% of accuracy while it reports 96.83% of trust validation score, which is notably higher in contrast to baselines.

Keywords: Artificial Intelligence, Federated Learning, Advanced Encryption Standard, Data Privacy, Auditing, distributed system

Introduction

The contribution of Artificial Intelligence (AI) is notably high towards various areas of healthcare system viz. personalized treatment planning, predictive analytics, intelligent disease diagnosis etc. However, there is a higher dependency of centralized data storage for classical AI-centric healthcare models that induce potential security complications like data leakage, data privacy, etc. One of the effective solution in such case is to adopt Federated Learning (FL) which can perform model training without need to share any data. However, FL models are also encountered with challenges which are mainly related to collaboration, trust, communication integrity.

Research Method

A novel trustworthy and secure healthcare diagnostic framework has been presented in proposed work integrating with Federated Learning (FL) where collaborative generation of clinical intelligence is carried out with decentralized auditing methods. Figure 1 showcase the architecture to represent that it offer transparent participation, secure sharing of models, and privacy preservation without disclosing any

sensitive information of patient among its healthcare partners. The complete work is classified into two core operational units i.e. *FL core module* and *Distributed Record Network-based validation module*. Both the modules carry out development and validation of secure healthcare model collaboratively.

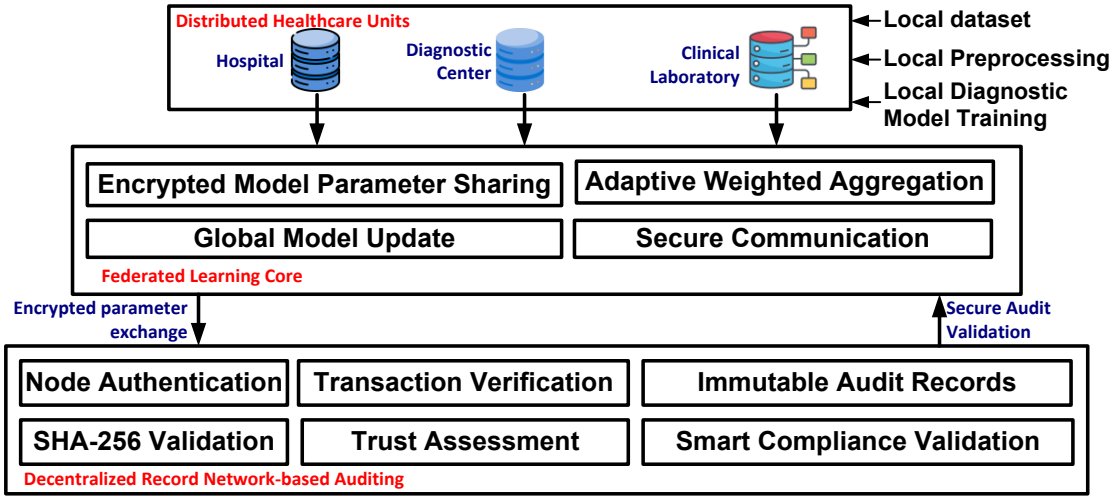


Figure 1. Architecture of Proposed Model

The operational modules are discussed as following:

- **FL-Core Module:** The module takes the input of clinical dataset from different healthcare units followed by performing preprocessing operation (viz. noise filtering, feature encoding, elimination of missing value, normalization, etc.). Private dataset is used by each healthcare unit to train local DL-based diagnostic model iteratively adopting local optimization function for minimizing prediction error. The system only transmits weight updates and encrypted model parameters to central fusion server and it doesn't share any raw records of healthcare. Various parameters like local data quality, training consistency, and institutional reliability are subjected adaptive weighted averaging by fusion server so that system can generate a potential diagnostic model. Further consecutive training rounds uses the updated global model while this mechanism is iterated till it reaches its convergence point. The output of this module is basically a diagnostic model that is globally optimized towards yielding precise prediction while retaining maximum level of distributed learning integrity and patient privacy.
- **Decentralized Record Network based Auditing**: This module takes the input of generated institutional transaction, aggregation records, authentication credentials, participation logs, and updates of encrypted model. The module initiates identity verification followed by authentication adopting consensus-centric validation in decentralized structure. Generated models are converted to immutable audit records while it also carry out assessment of institutional trust, update verification, and timestamp validation. For every round of communication, the decentralized network validates if the parameters of received model cater up to constraints of predefined integrity prior accepting for fusion. The output of this module is an audit trail that is both tampered resistant and verified while it consists of validated records of healthcare participation and authentical model transaction.

Result

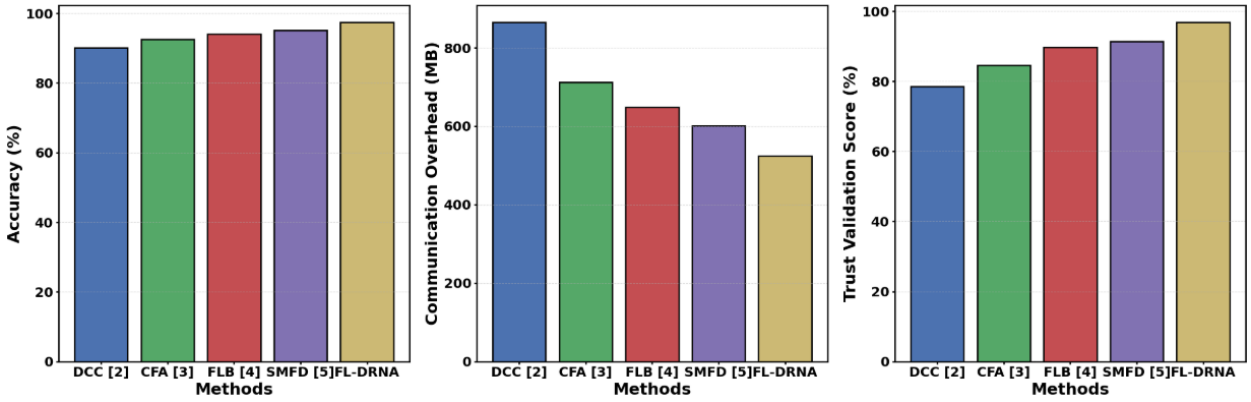
The proposed FL-DRNA has been scripted in python where specific DL libraries like PyTorch and TensorFlow has been used under 64-bit of normal Windows environment. MIMIC-III dataset has been adopted for this implementation as it consists records of multiple healthcare units with distributed patient diagnostic and clinical records [1]. Advanced Encryption Standard (AES-256) has been used towards securing the transmission by sharing the encrypted parameter resulting in secure aggregation method. From the perspective of hyperparameter adoption, FL-DRNA has used Adam optimizer with 0.001 as rate of learning, 32 as size of batch, 0.3 dropout ratio, 5 local epoch, and 100 rounds. This supports for resisting overfitting and optimized convergence. Further, SHA-256 has been used by decentralized auditing network towards preserving integrity and verifying transactions. Table 1 showcase the numerical outcome accomplished when proposed FL-DRNA is compared with four most frequently adopted models i.e., Diagnosis using Centralized CNN (DCC) [2], Classical Federated Averaging (CFA)[3], FL using Blockchain (FLB)[4], and Secure Multiparty Federated Diagnosis (SMFD)[5]. The assessment has been carried out with respect to accuracy, precision, communication overhead, and score of trust validation.

Table 1. Comparative Analysis Outcome

Method	Accuracy (%)	Precision (%)	Communication Overhead (MB)	Trust Validation Score (%)
DCC [2]	90.12	88.34	865	78.45
CFA[3]	92.48	90.17	712	84.63
FLB[4]	94.03	92.41	648	89.74
SMFD[5]	95.16	93.88	601	91.35
FL-DRNA	97.42	96.11	524	96.83

Discussion

Figure 2 showcase that FL-DRNA significantly excel better outcome in contrast to existing models of CCD, CFA, FLB, and SMFD. The implementation of decentralized auditing boosted the integrity and reliability of collaborative learning by verifying all institutional contributions and communication transactions via immutable process of verification.



(a) Accuracy (b) Communication Overhead (c) Trust Validation Score

Figure 2 Graphical Outcome of study

The outcome also showcased highly minimized communication overhead which is due to the fact that only encrypted model attributes were subjected to exchange while performing federated communication

while it doesn't transfer any form of patient information. Increased trust validation score by FL-DRNA also showcased its effectiveness while performing decentralized auditing towards collaboration of transparent healthcare system. CCD has higher dependency towards storage of centralized data while it also has increased vulnerability towards communication congestion and privacy leakage. CFA make use of very simplified attribute averaging without accounting for validation of malicious participants, data heterogeneity, institutional trust. FLB is noted with enhanced transparent transaction and yet its performance get adversely affected due to surplus latency and maximized computational complexity resulted by operations due to blockchain consensus. Finally, better results have been showcased by SMFD model and yet it lacks intelligent trust validation and adaptive decentralized auditing. This results in degradation of collaborative reliability along with cumulative efficiency in communication.

Conclusion

FL-DRNA is a collaborative model which emphasizes on data privacy. It has been noted that diagnostic accuracy has been significantly improved due to unification of decentralized auditing and adaptive federated aggregation. The system uses AES and immutable audit verification for improving transaction integrity and transparency. Experimental analysis shows that FL-DRNA excels better performance in contrast to existing methods that are frequently adopted. Future work will be carried out towards implementing fusion-based privacy preservation system by extending the current model followed by implementing Explainable AI (XAI) for enhanced clinical interpretability.

References

1. I. Aden, C. H. T. Child, and C. C. Reyes-Aldasoro, "International Classification of Diseases prediction from MIMIIC-III clinical text using pre-trained ClinicalBERT and NLP deep learning models achieving state of the art," Big Data Cogn. Comput., vol. 8, no. 5, p. 47, 2024, doi: 10.3390/bdcc8050047
2. S. Markkandan, N. P. G. Bhavani, and S. S. Nath, "A privacy-preserving expert system for collaborative medical diagnosis across multiple institutions using federated learning," Sci. Rep., vol. 14, no. 1, p. 22354, 2024, doi: 10.1038/s41598-024-73334-7
3. R. Abid, M. Rizwan, A. Alabdulatif, A. Alnajim, M. Alamro, and M. Azrour, "Adaptation of federated explainable artificial intelligence for efficient and secure E-healthcare systems," Comput. Mater. Contin., vol. 78, no. 3, pp. 3413–3429, 2024, doi: 10.32604/cmc.2024.046880
4. S. T. Ahmed et al., "Towards blockchain based federated learning in categorizing healthcare monitoring devices on artificial intelligence of medical things investigative framework," BMC Med. Imaging, vol. 24, no. 1, p. 105, 2024, doi: 10.1186/s12880-024-01279-4
5. C. Ying et al., "BIT-FL: Blockchain-enabled incentivized and secure federated learning framework," IEEE Trans. Mob. Comput., vol. 24, no. 2, pp. 1212–1229, 2025, doi: 10.1109/tmc.2024.3477616