AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

MEDILIGHT PRIVACY-AWARE EDGE-BASED DIAGNOSIS ASSISTANT FOR MOBILE HEALTHCARE

D. V.V. BHRAHMACHARI[1],
G. RANGANADHA RAO[2]
M-Tech Student, Dept.of CSE,**UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY**,Andhra pradhesh, India [1]
Associate Professor,Dept.of CSE,**UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY**,Andhra pradhesh, India[2] db.achari72@gmail.com ,
ranganath19@gmail.com

ABSTRACT:
With the rapid advancement of machine learning, mobile users can now submit their symptoms anytime and anywhere for instant medical assessment. To meet the low-latency requirements of real-time diagnosis services, edge computing has become a widely adopted solution. However, traditional data-driven machine learning models rely on large volumes of sensitive medical data, which raises serious privacy concerns. Therefore, ensuring strong privacy protection is essential.To address these challenges, this project introduces LPME, a lightweight privacy-preserving medical diagnosis framework designed for edge environments. LPME restructures the XGBoost model within an edge–cloud architecture by using encrypted model parameters instead of raw user data. This transformation significantly reduces the computational overhead by shifting most cipher text operations into efficient plain text operations, making the system suitable for resource-constrained edge devices. Additionally, LPME enables secure and private on-edge diagnosis, ensuring both timely responses and confidentiality of user information. Comprehensive security analysis and experimental results verify that LPME is secure, effective, and computationally efficient.

KEYTERMS: Medical,Assessment,Privacy,Edge–Cloud,Encrypted.

1 INTRODUCTION:

1.1 Introduction about the project

Machine learning is becoming increasingly important in modern medical diagnosis, enabling mobile users to submit their symptoms anytime and receive quick diagnostic feedback. Compared with traditional manual diagnosis—which often suffers from a shortage of medical experts and high costs—machine learning–based diagnosis offers significant advantages. It improves healthcare quality, reduces diagnostic expenses, and provides scalable solutions for large populations. As a result, the development of machine learning–driven medical diagnosis systems has gained considerable attention from both academic researchers and industry practitioners. With the rapid growth of telemedicine, the demand for intelligent healthcare services, clinical decision support, and mobile medical applications has risen sharply. However, this growth also brings several challenges, including limited availability of high-quality training data, system vulnerabilities, and increasing concerns about patient privacy.In real-world medical settings, collecting sufficient and well-labeled medical data is both costly and time-consuming. Individual medical institutions typically hold only small datasets, which are inadequate for building robust data-driven machine learning models. To train effective diagnostic models, it becomes essential to share and integrate distributed medical data across multiple organizations. With the advancement of cloud computing—which offers abundant storage and powerful computational capabilities—outsourcing medical data to the cloud has emerged as a popular approach for training large-scale machine learning models

2 LITERATURE SURVEY:

2.1. Problem context

Mobile healthcare applications and wearable sensing devices continuously collect sensitive personal health information, including symptoms, vital signs, ECG/PPG signals, and medical images. Transmitting this raw data directly to the cloud introduces several challenges, such as privacy risks, communication delays, and dependency on stable network connectivity. To address these issues, edge-based diagnostic systems perform data processing closer to the user—either on the device itself or on a nearby edge gateway. This approach significantly reduces latency, enhances privacy protection, and minimizes bandwidth usage.Recent reviews in the field of edge AI for healthcare emphasize its strong potential to support real-time diagnostic services and intelligent monitoring. However, they also point out key challenges that must be addressed before widespread adoption becomes feasible. These include ensuring robust privacy-preserving mechanisms, compressing models to fit resource-constrained edge devices, and establishing trust in edge-based decision systems.

2.2. Data, evaluation & benchmarks

Medical AI systems depend heavily on clinically validated datasets such as ECG recordings, chest X-ray images, and symptom logs. Their performance is usually assessed using established clinical metrics, including sensitivity (recall), specificity, and AUC. In addition to diagnostic accuracy, system-level metrics—such as inference latency, energy consumption, and bandwidth usage—are essential for evaluating real-world feasibility. Privacy-preserving techniques introduce another layer of evaluation, requiring disclosure of privacy budgets (e.g., ε in differential privacy), while federated learning approaches typically report communication rounds and model convergence behavior. Therefore, MEDILIGHT must demonstrate effectiveness across both dimensions: high-quality diagnostic performance and minimal privacy or system overhead.

2.3. Privacy-preserving methods relevant to MEDILIGHT

2.3.1. Differential Privacy (DP).

DP ensures formal privacy guarantees by injecting calibrated noise into model updates or outputs. Although effective, balancing privacy strength and model accuracy demands careful tuning—especially in medical diagnostics where precision is critical.

2.3.2. Secure Multi-Party Computation (MPC) and Homomorphic Encryption (HE).

These cryptographic techniques allow computation over encrypted data. While highly secure, their computational overhead can be heavy for small edge devices. As a result, hybrid designs often offload intensive encrypted computation to gateways or cloud servers.

2.3.3. Trusted Execution Environments (TEEs).

Hardware-backed enclaves such as Intel SGX and ARM TrustZone provide a practical middle ground, enabling secure execution of sensitive operations on edge servers while maintaining reasonable performance.

3 EXISTING SYSTEM

In real-world medical settings, collecting sufficient and well-labeled medical data is both costly and time-consuming. Individual medical institutions typically hold only small datasets, which are inadequate for building robust data-driven machine learning models. To train effective diagnostic models, it becomes essential to share and integrate distributed medical data across multiple organizations. With the advancement of cloud computing—which offers abundant storage and powerful computational capabilities—outsourcing medical data to the cloud has emerged as a popular approach for training large-scale machine learning models

DIS ADVANTAGES:

1) To meet the low-latency requirements of real-time diagnosis services, edge computing has become a widely adopted solution.

2) Traditional data-driven machine learning models rely on large volumes of sensitive medical data, which raises serious privacy concerns.

4 PROPOSED SYSTEM

To overcome the challenges identified earlier, this work introduces a lightweight, privacy-preserving variant of XGBoost that operates over encrypted model parameters, significantly reducing computational burden compared with traditional data-sharing–based privacy-preserving machine learning. We present the Lightweight Privacy-Preserving Medical Diagnosis Framework for Edge Computing (LPME), which consists of three key components:

1. Lightweight XGBoost on Edge.

LPME constructs an XGBoost diagnostic model using encrypted model parameters trained collaboratively across multiple edge devices instead of relying on raw training data. This design avoids the overhead of storing and managing large volumes of medical data at edge nodes while ensuring that XGBoost remains practical and effective in distributed environments.

2. Privacy-Preserving Training.

To safeguard sensitive information during training, LPME employs a homomorphic-encryption-based secure computation mechanism using a single-cloud architecture. The secret key is split into two random shares, and only one share is stored in the cloud. This prevents the cloud from recovering plaintext parameters while still allowing it to perform encrypted computations and select optimal model parameters. The approach offers strong privacy guarantees while remaining feasible for resource-constrained edge devices.

3. Secure XGBoost-based Diagnosis at the Edge.

For inference, LPME enables users to submit encrypted symptom data to nearby edge nodes, which compute the diagnosis results over encrypted inputs. Homomorphic encryption ensures that both the user's query and the diagnostic outcome remain confidential. The edge node then returns the encrypted prediction, providing secure and low-latency diagnosis suitable for real-time medical applications.

ADVANTAGES

1) LPME system provides secure diagnosis, in which a mobile user can submit his/her encrypted requests to an edge, then the edge will return the corresponding diagnosis results.

2) During the process, HE is adopted to guarantee confidentiality of the returned diagnosis results for implementing the private and timely diagnosis.

5. SYSTEMARCHITECTURE:

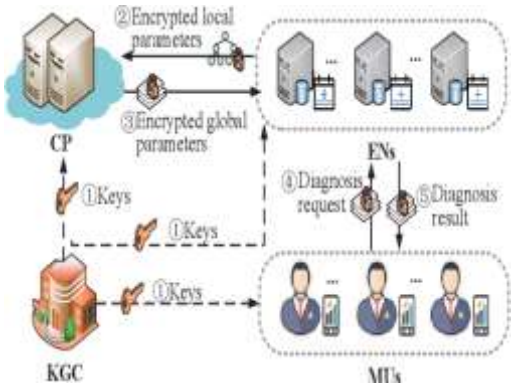

Fig1:System Architecture

6 RELATED WORK:

6.1 Edge AI and On-Device Medical Inference

Research in edge computing for healthcare highlights the importance of performing inference directly on mobile devices, wearables, or nearby gateways. This approach minimizes latency, protects data locality, and reduces bandwidth usage—critical for real-time biomedical monitoring. Advances in lightweight neural architectures, along with compression techniques such as quantization, pruning, and knowledge distillation, enable efficient execution of ECG/PPG analysis and image-based diagnostics on resource-constrained hardware. These methods form the

foundation of MEDILIGHT, which conducts initial triage, feature extraction, and early diagnosis at the device or gateway before any cloud involvement, thereby improving responsiveness and privacy.

6.2 Federated Learning and Collaborative Privacy-Preserving Training

Federated Learning (FL) has emerged as a leading solution for training medical AI models collaboratively without centrally aggregating raw patient data. FL frameworks designed for healthcare address key challenges such as device heterogeneity, non-IID data distributions, intermittent connectivity, and compliance with privacy regulations. Recent studies further integrate secure aggregation protocols and communication-efficient updates to support deployment on mobile phones and wearables. MEDILIGHT can exploit FL to continuously refine diagnostic models while ensuring that each user's data remains stored locally on their own device.

6.3Differential Privacy, Homo-morphemic Encryption, and Secure Aggregation

To safeguard model updates and inference outputs, the literature proposes a variety of privacy-enhancing technologies. Differential Privacy (DP) provides mathematically grounded guarantees against information leakage, whereas Homomorphic Encryption (HE) and secure aggregation protocols protect contributions from being exposed during federated model updates. Although DP may reduce model accuracy and HE can impose significant computational overhead, hybrid approaches—such as selectively applying DP or performing encrypted aggregation on trusted gateways—have shown to effectively balance utility and privacy. These strategies are directly relevant to MEDILIGHT, which must design a learning pipeline that prioritizes confidentiality without compromising diagnostic performance.

6.4 Trusted Execution Environments (TEEs) and Confidential Computing

Trusted Execution Environments, including Intel SGX and ARM TrustZone, are widely explored as practical mechanisms for executing sensitive computations—such as model aggregation, secure decryption, and private analytics—in hardware-isolated enclaves. TEEs reduce reliance on heavy cryptographic techniques, offering a more efficient environment for certain privacy-critical operations. In MEDILIGHT, TEEs can support secure edge-gateway processing, enabling private model-update aggregation or more computationally demanding diagnostic routines. Recent research, however, also identifies potential attack vectors on TEEs, reinforcing the need for a defense-in-depth approach that combines hardware isolation with cryptographic protections.

7 RESULTS:

In above screen first column showing original dataset and second column showing encrypted format of that original plain data and now dataset is encrypted and now click on 'Train Encrypted Data with XGBoost' link to train dataset and to build XGBOOST secure disease prediction model.

In above screen in first column you can see

then encrypted test data and in second column you can see prediction result as 'No Heart Disease Detected' or 'Heart Disease Detected'

8 CONCLSUION

The proposed project introduces a lightweight, privacy-preserving XGBoost framework designed specifically for edge environments. The framework enables efficient model construction across edge nodes while ensuring strong privacy protection, allowing sensitive medical data to remain secure throughout the process. Through secure computation techniques, the LPME system builds XGBoost models with minimal computational overhead and delivers fast, privacy-aware medical diagnosis directly at the edge. Experiments conducted on real-world medical datasets demonstrate that LPME achieves both high diagnostic performance and robust privacy guarantees, confirming its suitability for real-time healthcare applications in edge computing environments.

9 REFERENCES

[1] X. Wang, J. Ma, Y. Miao, X. Liu, and R. Yang, "Privacy-preservingdiverse keyword search and online pre-diagnosis in cloud computing," IEEE Transactions on Services Computing, 2019.

[2] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDeep:An efficient and secure duplication scheme for cloud-assistedehealth systems," IEEE Trans. Industrial Informatics, vol. 14, no. 9,pp. 4101–4112, 2018.

[3] B. Fu, P. Liu, J. Lin, L. Deng, K. Hu, and H. Zheng, "Predictinginvasive disease-free survival for early-stage breast cancer patientsusing follow-up clinical data," IEEE Transactions on BiomedicalEngineering, 2018.

[4] A. Galletta, L. Carnevale, A. Bramanti, and M. Fazio, "An innovative methodology for big data visualization for telemedicine,"IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 490497, 2018.

[5] I. Kononenko, "Machine learning for medical diagnosis: historystate of the art and perspective," Artificial Intelligence in medicine,vol. 23, no. 1, pp. 89–109, 2001.

[6] C. P. Friedman, A. K. Wong, and D. Blumenthal, "Achieving anationwide learning health system," Science Translational Medicine,vol. 2, no. 57, pp. 57cm29–57cm29, 2010.

[7] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, H. Wu, and H. Li, "Fairand dynamic data sharing framework in cloud-assisted internet ofeverything," IEEE Internet of Things Journal, 2019.

[8] Y. Miao, Q. Tong, K.-K. R. Choo, X. Liu, R. H. Deng, and H. Li,"Secure online/offline data sharing framework for cloud-assistedindustrial internet of things," IEEE Internet of Things Journal, 2019.

[9] Y. Miao, J. Weng, X. Liu, K.-K. R. Choo, Z. Liu, and H. Li, "Enablingverifiable multiple keywords search over encrypted cloud data,"Information Sciences, vol. 465, pp. 21–37, 2018.

[10] T. Ouyang, R. Li, X. Chen, Z. Zhou, and X. Tang, "Adaptiveuser-managed service placement for mobile edge computing: Anonline learning approach," in Proc. IEEE Conference on ComputerCommunications (INFOCOM'19). IEEE, 2019, pp. 1468–1476.

[11] P. Dai, K. Liu, X. Wu, H. Xing, Z. Yu, and V. C. Lee, "A learningalgorithm for real-time service in vehicular networks with mobileedge computing," in Proc. IEEE International Conference on Communications (ICC'19). IEEE, 2019, pp. 1–6.

[12] F. Wang, C. Zhang, J. Liu, Y. Zhu, H. Pang, L. Sun et al., "Intelligentedge-assisted crowdcast with deep reinforcement learning forpersonalized qoe," in Proc. IEEE Conference on Computer Communications (INFOCOM'19). IEEE, 2019, pp. 910–918.

FIRST AUTHORS:

D.V.V. BHRAHMACHARI Completed in Master of Computer Applications(MCA) and pursuing his M.Tech in Computer Science And Engineering in Universal College Of Engineering And Technology.

SECOND AUTHOR:

G. RANGANADHA RAO,M.Tech and B.Tech received his degree's in computer science and engineering. He is currently working as a Associate Professor of CSE in Universal College Of Engineering And Technology.