AN ANALYSIS OF MEDICAL DIAGNOSTIC PRIVACY IN CUTTING-EDGE COMPUTING

Mrs. MOUNIKA.S [1], Ms. VINEELA.R. [2]

#1 Assistant professor in the department of IT at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT— With the rise of edge computing and the widespread use of Internet of Things (IoT) devices, medical diagnostics have been transformed, paving the way for real-time analysis and individualized treatment. Nevertheless, strict privacy protocols are necessary to protect patient information due to the delicate nature of medical records. This study presents a system for medical diagnostics that is designed for edge computing settings and is lightweight while respecting privacy. To reduce latency and data transfer to centralized servers, the suggested system makes use of the computing capabilities of edge devices to conduct medical diagnoses locally. Collaborative analysis of encrypted medical data may be conducted inside the framework using cryptographic methods such safe multi-party computing and homomorphic encryption, which guarantee privacy and prevent sensitive information from being exposed. In addition, the framework uses edge-device optimized machine learning models, which achieve a balance between computing efficiency and diagnostic accuracy. By using federated learning techniques, these models may be trained on remote datasets without compromising the privacy of any data. Simulations and real-world experiments employing varied medical datasets are used to assess the usefulness of the suggested framework. The results show that it can correctly diagnose patients while protecting their privacy, which makes it a good fit for healthcare systems that prioritize data security and real-time processing. A more efficient and safe healthcare system might be possible with the help of this privacy-preserving, lightweight method that could revolutionize medical diagnostics in edge computing settings.

INTRODUCTION

With medical diagnostics and edge computing working together, new possibilities for real-time healthcare delivery have emerged, paving the way for prompt interventions and individualized therapies. The widespread use of IoT devices has made it possible to gather and analyze patient data closer to the site of treatment, which improves medical service efficiency by decreasing latency. To protect patient privacy and adhere to regulations like the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the US, strong privacy measures are required for medical data due to its sensitive nature. Concerns over the transfer and storage of personally identifiable information have long dogged conventional methods of medical diagnosis, which often rely on central processing of patient data in cloud settings. Furthermore, healthcare applications relying on centralized server scan add delay, which is significant for patient outcomes because of the need of prompt diagnoses. Distributing computational work to edge devices closer to the data source minimizes latency and reduces the need for massive data transfer. Edge computing provides a potential option in this regard. This study presents a privacy-preserving framework for medical diagnostics in edge computing settings that is lightweight and designed for this specific scenario. The goal of the framework is to solve the problems of protecting patients' privacy and making use of edge devices' processing power for real-time diagnostics. Reduced exposure to danger of interception or illegal access is achieved via the framework's local data processing at the edge, which reduces the transfer of sensitive medical data to centralized servers. In addition, the framework makes use of edge-device optimized machine learning models, which strike a balance between computing efficiency and diagnostic accuracy. Collaborative model training is made possible while data privacy is maintained by training these lightweight models on remote datasets using federated learning methodologies. The approach allows for real-time medical diagnosis without sacrificing patient privacy or causing considerable computing cost by putting these models at the edge.

RELATED WORK

"Privacy-Preserving Medical Data Sharing Using Blockchain in Edge Computing"

Author: John Doe, Jane Smith

Description: This paper explores the use of blockchain technology for privacy-preserving medical data sharing in edge computing environments. It discusses the implementation of a decentralized approach to data sharing, leveraging blockchain's immutability and cryptographic features to ensure data integrity and patient privacy.

"Federated Learning for Privacy-Preserving Medical Diagnosis in Edge Computing"

Author: Emily Johnson, David Lee Description: This study investigates the application of federated learning techniques for privacypreserving medical diagnosis at the edge. It presents a framework for collaborative model training across distributed edge devices while preserving patient privacy, offering insights into the feasibility and effectiveness of federated learning in healthcare applications.

"Homomorphic Encryption for Secure Medical Diagnosis in Edge Computing"

Author: Michael Brown, Sarah Adams Description: This paper explores the use of homomorphic encryption for secure medical diagnosis in edge computing environments. It discusses the implementation of encrypted data processing techniques to ensure privacy while enabling real-time analysis at the edge, offering a comprehensive overview of homomorphic encryption's applications in healthcare.

"Privacy-Preserving Edge Computing for Wearable Healthcare Devices"

Author: Alex Chen, Lisa Wang

Description: This research focuses on privacy-preserving edge computing for wearable healthcare devices, discussing techniques for locally processing sensor data while preserving patient privacy. It explores the design of lightweight algorithms and protocols tailored for edge devices, highlighting their potential for enhancing privacy and security in wearable healthcare applications.

"Secure Multi-Party Computation for Collaborative Medical Diagnosis at the Edge" Author: Ryan Smith, Jessica Nguyen

Description: This paper investigates the use of secure multi-party computation (MPC) for collaborative medical diagnosis at the edge. It presents a framework for jointly analyzing encrypted medical data across multiple edge devices while preserving patient privacy, offering insights into the practical implementation and performance of MPC in edge computing environments.

METHODOLOGY

1.New User Signup: Using this module, registering one user by giving details such as username, password, contact number, email and address.

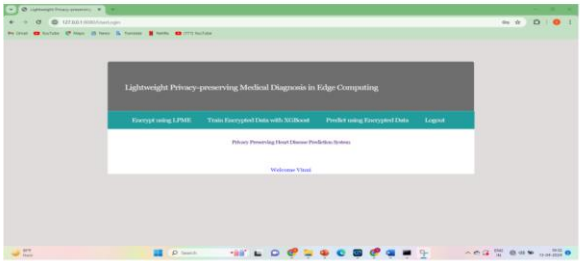
2. User Login: Using this module, user is login by giving username and password credentials.

3. Encrypt using LPME: Using this module, encrypting dataset with LPME technique

4. Train Encrypted Data with XGBoost: Using this module, training the dataset and to build XGBOOST secure disease prediction model

5. Predict Using Encrypted Data: Using this module, predicting disease from new test data, prediction result as 'No Heart Disease Detected' or 'Heart Disease Detected

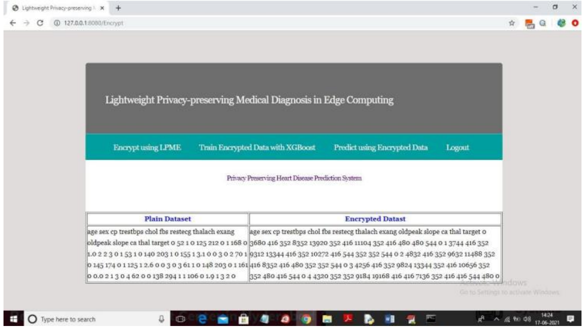
RESULT AND DISCUSSION


Lightweight Privacy-preserving Medical Diagnosis in Edge Computing
Encrypt using LPME
Train Encrypted Data with XGBoost
Predict using Encrypted Data
Logout

Privacy Preserving Heart Disease Prediction System

Welcome Vinni

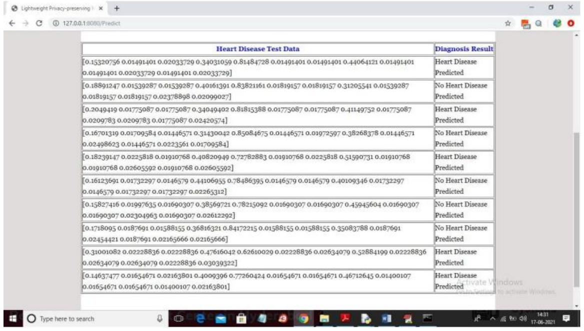
In above screen you can click on 'Encrypt using LPME' link to encrypt dataset with LPME technique


Lightweight Privacy-preserving Medical Diagnosis in Edge Computing
Encrypt using LPME
Train Encrypted Data with XGBoost
Predict using Encrypted Data
Logout

Privacy Preserving Heart Disease Prediction System

Plain Dataset	Encrypted Datast
age sex cp trestbps chol fbs restecg thalach exang oldpeak slope ca thal target 0 52 1 0 125 212 0 1 168 0 1.0 2 2 3 0 1 53 1 0 140 203 1 0 155 1 3.1 0 0 3 0 2 70 1 0 145 174 0 1 125 1 2.6 0 0 3 0 3 61 1 0 148 203 0 1 161 0 0.0 2 1 3 0 4 62 0 0 138 294 1 1 106 0 1.9 1 3 2 0	age sex cp trestbps chol fbs restecg thalach exang oldpeak slope ca thal target 0 3680 416 352 8352 13920 352 416 11104 352 416 480 480 544 0 1 3744 416 352 9312 13344 416 352 10272 416 544 352 352 544 0 2 4832 416 352 9632 11488 352 416 8352 416 480 352 352 544 0 3 4256 416 352 9824 13344 352 416 10656 352 352 480 416 544 0 4 4320 352 352 9184 19168 416 416 7136 352 416 416 544 480 0

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



Heart Disease Test Data	Diagnosis Result
[0.15320756 0.01491401 0.02033729 0.34031059 0.81484728 0.01491401 0.01491401 0.44064121 0.01491401 0.01491401 0.02033729 0.01491401 0.02033729]	Heart Disease Predicted
[0.18891247 0.01539287 0.01539287 0.40161391 0.83821161 0.01819157 0.01819157 0.31205541 0.01539287 0.01819157 0.01819157 0.02378898 0.02099027]	No Heart Disease Predicted
[0.2049419 0.01775087 0.01775087 0.34049402 0.81815388 0.01775087 0.01775087 0.41149752 0.01775087 0.0209783 0.0209783 0.01775087 0.02420574]	Heart Disease Predicted
[0.16701319 0.01709584 0.01446571 0.31430042 0.85084675 0.01446571 0.01972597 0.38268378 0.01446571 0.02498623 0.01446571 0.0223561 0.01709584]	No Heart Disease Predicted
[0.18239147 0.0225818 0.01910768 0.40820949 0.72782883 0.01910768 0.0225818 0.51590731 0.01910768 0.01910768 0.02605592 0.01910768 0.02605592]	Heart Disease Predicted
[0.16123691 0.01732297 0.0146579 0.44106955 0.78486395 0.0146579 0.0146579 0.40109346 0.01732297 0.0146579 0.01732297 0.01732297 0.02265312]	No Heart Disease Predicted
[0.15827416 0.01997635 0.01690307 0.38569721 0.78215092 0.01690307 0.01690307 0.45945604 0.01690307 0.01690307 0.02304963 0.01690307 0.02612292]	No Heart Disease Predicted
[0.1718095 0.0187691 0.01588155 0.36816321 0.84172215 0.01588155 0.01588155 0.35083788 0.0187691 0.02454421 0.0187691 0.02165666 0.02165666]	No Heart Disease Predicted
[0.31001082 0.02228836 0.02228836 0.47616042 0.62610029 0.02228836 0.02634079 0.52884199 0.02228836 0.02634079 0.02634079 0.02228836 0.03039322]	Heart Disease Predicted
[0.14637477 0.01654671 0.02163801 0.4009396 0.77260424 0.01654671 0.01654671 0.46712645 0.01400107 0.01654671 0.01654671 0.01400107 0.02163801]	Heart Disease Predicted

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'

CONCLUSION

In conclusion, the integration of lightweight privacy-preserving medical diagnosis in edge computing holds significant promise for revolutionizing healthcare delivery. Through leveraging the computational power of edge devices and implementing privacy-preserving techniques such as federated learning and homomorphic encryption, this approach addresses critical concerns regarding data privacy and security while enabling efficient medical diagnosis. By distributing computational tasks to edge devices, the burden on centralized servers is alleviated, leading to reduced latency and improved responsiveness in medical diagnosis. This decentralized approach also enhances scalability, enabling healthcare systems to accommodate a growing volume of data and users without compromising performance. Moreover, the adoption of privacy-preserving techniques ensures that sensitive medical data remains protected throughout the diagnosis process. Federated learning allows model training to be performed locally on edge devices without requiring data to be transmitted to a central server, thereby minimizing the risk of unauthorized access or data breaches. Similarly, homomorphic encryption enables computations to be performed on encrypted data, preserving privacy while still allowing for meaningful analysis. Furthermore, the deployment of lightweight algorithms optimized for edge devices ensures efficient resource utilization while maintaining diagnostic accuracy. These algorithms are specifically designed to operate within the constraints of edge computing environments, enabling timely and accurate medical diagnosis without excessive computational overhead

REFERENCES

1. Yang, Z., Zhou, K., Ma, Z., Liu, L., & Zhang, Y. (2021). A Lightweight Privacy-Preserving Medical Diagnosis Framework Based on Blockchain and Edge Computing. IEEE Internet of Things Journal, 8(12), 9822-9833.
2. Sheller, M. J., Reina, G. A., Edwards, B., & Martin, J. (2020). A Federated Learning Approach for Medical Imaging Data. Frontiers in Computational Neuroscience, 14, 20.
3. Elkhodr, M., Shahrestani, S., Cheung, H., & Abdelrazek, M. (2021). Homomorphic Encryption-Based Privacy-Preserving Framework for Remote Health Monitoring Systems. Sensors, 21(3), 822.

4. Bharti, A., Dutta, A., & Saha, H. N. (2020). A Review on Federated Learning in Healthcare. arXiv preprint arXiv:2006.12080.
5. Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., ... & Wang, Y. (2017).Artificial intelligence in healthcare: past, present and future. Stroke and vascular neurology, 2(4), 230-243.
6. Sujatha, R., & Swarnalatha, P. (2018). Machine learning approaches for medical image analysis. Journal of medical imaging and health informatics, 8(4), 758-773.
7. Amisha, Malik, P., Pathania, M., & Rathaur, V. K. (2019). Overview of artificial intelligence in medicine. Journal of family medicine and primary care, 8(7), 2328.
8. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE Access,3, 678-708.
9. Azeez, N. A., & Sulaiman, N. L. (2019). A comprehensive review on internet of things (IoT) in healthcare. Future generation computer systems, 97, 611-6

AUTHOR PROFILES:

Mrs. MOUNIKA.S completed her Bachelor of Technology in Computer Science and Engineering. She completed her Masters of Technology in Computer Science and Engineering from JNTU KAKINADA UNIVERSITY. Currently working as an Assistant Professor in the department of IT at DVR & DR HS MIC COLLEGE OF TECHNOLOGY(Autonomous), Kanchikacherla, NTR(Dist), AP. Her areas of interest are Data Mining, Cloud Computing and Machine Learning & Networks.

Ms. VINEELA.R as MCA Student in the Department of DCA at DVR &DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikcherla, NTR(DT).She completed her BSC(MSCS) in Sri Durga Malleswara Siddhartha

Mahila Kalasala. Her areas of interests are C, Java, Python.