Versatility of Homomorphic Encryption Scheme within Healthcare Implementations

Eric Yang, Dr. Zhiyuan Yan

Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA

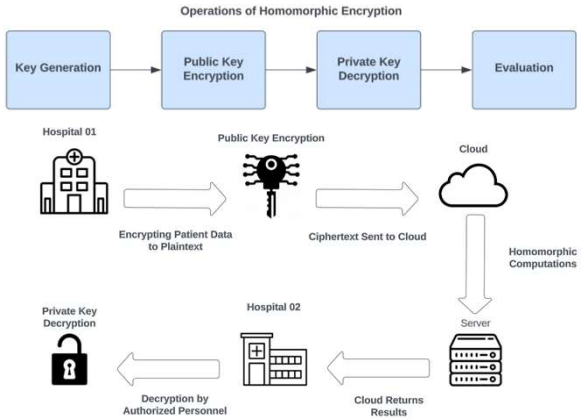
INTRODUCTION

Homomorphic encryption allows data to be transformed into encrypted form while still enabling mathematical operations to be performed directly on the encrypted data, without the need for decryption.

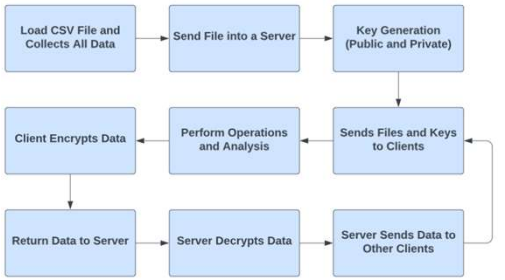
The purpose of this project is to provide a potential solution to combat the loss of patient privacy when their most valuable information are inputted into the healthcare system. Patients often lack control over their data once it enters the cloud, exposing them to risks such as malicious insiders, data breaches, and insecure interfaces. To address these challenges, implementing homomorphic encryption could provide a robust solution. This encryption technique allows for the collection and sharing of patient data across various locations while maintaining privacy and security. By integrating these technologies, healthcare providers can bolster data security, streamline operations, and ultimately enhance patient care.

BACKGROUND

- Sensitive information remains safeguarded throughout processing, ensuring privacy and security.
- Offers a flexible and secure method for processing sensitive information, preserving confidentiality while allowing for essential computations to be performed



METHODOLOGY

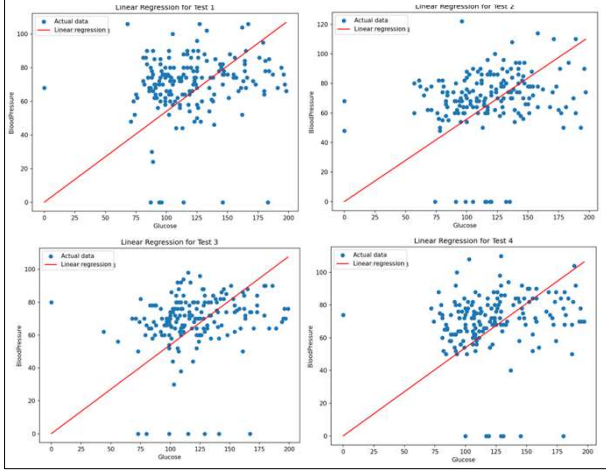


The simulation code executes a process where each client represents a "hospital." Loop ends when the last client takes in the data.

RESULTS

Comparison of Correlation between Lifestyle Impacts and Factors

Name of Dataset	X Value	Y Value	MSE	Correlation Coefficient
GHSH_Pooled_Data1	Smoke_cig_currently	Attempted_Suicide	100.61	0.2438
Sleep_health_and_lifestyle	Sleep Duration	Stress Level	8.84	-0.7919
diabetes	Glucose	BloodPressure	379.79	0.1425



Health data from multiple datasets, sourced from Kaggle, undergo horizontally partitioned learning to maintain patient privacy. This process involves strict privacy constraints that confine records within individual clients and encrypt shared information. Collaboratively, linear regression with gradient descent is utilized in the model-building process, ensuring the safeguarding of sensitive patient information.

In this simulation, each client performs correlation analysis on the same dataset, focusing on variables like Glucose and Blood Pressure. The correlation analysis results from each client are then averaged to compute a final correlation coefficient. This coefficient, along with Mean Squared Error (MSE), is displayed in a table showcasing the performance of different datasets in the model-building process.

CONCLUSION

- Successfully perform correlation analysis and Mean Squared Error onto encrypted data
- Patient data is secured and never compromised between each client.
- Promising solution for data security and privacy, especially in healthcare.
- Health professionals can leverage encryption schemes to predict lifestyle factors and health triggers.

FUTURE WORK

- Optimized algorithms and enhanced efficiency expected to make homomorphic encryption more accessible.
- Transformative applications anticipated in secure health data sharing, analytics, and collaborations.
- Expected role of homomorphic encryption in revolutionizing healthcare practices by providing robust data security.

ACKNOWLEDGEMENT

David and Lorraine Freed Undergraduate Research Symposium, Lehigh University

LEHIGH UNIVERSITY | P.C. Rossin College of Engineering and Applied Science

DAVID AND LORRAINE FREED UNDERGRADUATE RESEARCH SYMPOSIUM

LEHIGH ELECTRICAL AND COMPUTER ENGINEERING

REFERENCES

- A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam and T. Soyata, "Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms," 2014 IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA, 2014, pp. 48-52, doi: 10.1109/GLOCOMW.2014.7063384.
- Acar, Abbas, et al. "A survey on homomorphic encryption schemes." *ACM Computing Surveys*, vol. 51, no. 4, 2018, pp. 1–35, https://doi.org/10.1145/3214303.
- Alloghani, Mohamed, et al. "A systematic review on the status and progress of Homomorphic Encryption Technologies." *Journal of Information Security and Applications*, vol. 48, 2019, p. 102362, https://doi.org/10.1016/j.jisa.2019.102362.
- Bos, Joppe W., et al. "Private predictive analysis on encrypted medical data." *Journal of Biomedical Informatics*, vol. 50, 2014, pp. 234–243, https://doi.org/10.1016/j.jbi.2014.04.003.