International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Medical Data Privacy Using Homomorphic Encryption

Aman Kumar[1], Akash Yadav[2], Dr. Gousiya Begum[3], Ms. P. Poornima[4]

[1,2]Student, Department of Computer Science Engineering, MGIT
[3,4]Assistant Professor, Department of Computer Science Engineering, MGIT,

Abstract

The digitalization of healthcare information raises serious issues of privacy and security. Classical encryption needs to be decrypted in order to analyze, leaving confidential data vulnerable to compromise. Homomorphic encryption is used in this project to allow computation on encrypted medical information without decryption, thereby preserving privacy from data creation to usage. Built with healthcare in mind, the system supports secure analysis and exchange of data without breaching confidentiality. Our approach targets algorithm efficiency, system integration, and scalability for supporting privacy-protecting healthcare analytics.

Keywords: Homomorphic Encryption, Data Security, Healthcare Data.

1. Introduction

Security of sensitive health information has been among the essential concerns of contemporary digital living. Digitization of medical background at high speed and dependency on data analysis for healthcare necessitate increased caution regarding patient-related information. Encrypted data is secure when it remains undecrypted, but without it, analysis cannot be carried out, and therefore the data becomes exposed to potential invasion and misuse. This problem requires the creation of new cryptographic methods that maintain data privacy without losing data utility [1].

Homomorphic encryption presents a solution to this problem. It is a sophisticated method of cryptography that enables computations on encrypted data without decrypting it beforehand. This ability ensures sensitive medical data stays protected during its processing life cycle. Healthcare data is very valuable and sensitive. Therefore, it requires robust protection mechanisms. Homomorphic encryption and federated learning provide a robust architecture for secure data analysis. It allows various institutions to train their machine learning models on common data without exposing the underlying datasets. This homomorphically encrypted federated learning architecture maintains high classification accuracy and data utility while guaranteeing privacy [2].

Fully Homomorphic Encryption (FHE) has been acknowledged as a game-changer in data security and trust in the IT industry ever since its theoretical discovery by Craig Gentry in 2009. FHE has since then been made more practical and efficient and, hence, has been an opportunity to use it in various fields like health care [3].

Practical uses of homomorphic encryption extend beyond theoretical uses. It is especially effective for secure data exchange and collaborative research, where data privacy is of utmost importance. In cryptographic computing, homomorphic encryption allows computations on encrypted data securely, and hence it is effective in applications that require high confidentiality [3].

Another security layer added to healthcare data exchange is achieved by integrating homomorphic encryption with fog computing. The approach is associated with storage and computation overheads well taken care of utilizing fog nodes to provide secure processing of data dealing with leakage as well as access control issues [4].

Remote Health Monitoring has come up as a field of promise for the extension of health to remote and disadvantaged areas. Fully homomorphic encryption ensures confidentiality of patient information while enabling health status reporting and monitoring through adaptive autonomous protocols. This adaptive protocol is tested by cloud-based machine learning models across various types of patient conditions and turned out to be practical and effective [4].

Lastly, the integration of Secure Multiparty Computation (MPC) and homomorphic encryption provides a cost-effective and secure solution to e-healthcare systems. This system is especially appropriate during the COVID-19 pandemic; it allows remote healthcare provision while securely sharing and processing patient data. With the integration of MPC and homomorphic encryption, this system enhances data security and scalability for future use [5].

Homomorphic encryption plays a crucial role in health care by enabling secure cloud storage and data sharing. It enables complex calculations on encrypted data while enabling research collaboration and the creation of data-driven decisions without compromising patient privacy. The underlying cryptography increases the security in cloud computing by reducing many of the threats associated with traditional methods of data processing [6].

A systematic review confirms these benefits and highlights homomorphic encryption's growing importance in the healthcare industry [7]. Homomorphic encryption with DLT increases data security through preservation of data privacy during computation and permanent retention of all data transfer and processing operations. This makes integrity of data preserved and full audits accessible for conformity with data protection and research ethics protocols [8].

New technologies in data security will emerge through the integration of homomorphic encryption with new technologies like AI/ML models in hybrid clouds. It preserves accuracy and efficiency in AI models and adheres to strict compliances like HIPAA and GDPR. Though the implementation process is complex, there is great potential for the application of homomorphic encryption in protecting patient data in contemporary healthcare systems [9].

Finally, integrating Secure Multiparty Computation (MPC) and homomorphic encryption provides a reliable and effective solution to e-healthcare systems. The model supports remote healthcare services along with securely sharing and processing patient data. By integrating MPC and homomorphic encryption, the method enhances data security and future-proof scalability for healthcare applications [10].

2. Review of Related Works

Fully Homomorphic Encryption (FHE) has drawn enormous interest in secure computation. A detailed survey by Armknecht et al. offers an elementary introduction to FHE, presenting definitions, real-world

applications, and the threat of its high computational cost. Though providing an in-depth view of terminology and concepts, the paper highlights the security-performance trade-off in practical application [1].

Wang et al. built upon this by introducing a privacy-preserving federated learning scheme based on homomorphic encryption. Their solution successfully safeguards the model training procedure using encryption and incorporates access control and acknowledgment methods. With strong utility and classification accuracy, its complicated process of implementation may deter adoption [2].

Orlandi and Scholl's work brings out the promise of homomorphic encryption in overall cryptographic computing. It stresses the significance of secure computation on encrypted data but points out that its applicability range is still confined to certain fields. Nevertheless, it is a useful manual for incorporating encryption in cryptographic systems [3].

Sheu et al. introduced an adaptive protocol—AutoPro-RHC—that is designed to be used for remote healthcare monitoring. The protocol uses fully homomorphic encryption to preserve data confidentiality while generating real-time patient reports. Developed based on TFHE libraries and implemented on the AWS cloud, the model is strong in adaptability but might be plagued by high resource usage, which could restrict its large-scale deployment [4].

Lamia gives a broad overview of homomorphic encryption in healthcare, specifically its application in secure cloud storage, data sharing, and collaborative medical research. Although the paper emphasizes its revolutionary potential in personalized medicine and remote monitoring, it does not have practical case studies that would make it more applicable in real-world scenarios [5].

Scheibner et al. discuss incorporating homomorphic encryption and distributed ledger technologies in safe patient data sharing. From the qualitative evaluations of Swiss hospitals, they discuss how the approach supports ethical and legal compliance. Though strong, the paper calls for cautious consideration of the ethical issues at deployment [6].

A systematic review by Munjal and Bhatia outlines the history of homomorphic encryption in the healthcare sector. Though enlightening, the review is largely theoretical in nature and devoid of tangible implementation approaches, thereby making it of less use for developers and practitioners who seek to achieve practical incorporation [7].

Kummarapurugu suggests protecting AI/ML pipelines in hybrid cloud settings through homomorphic encryption. This framework is HIPAA and GDPR compliant and provides a strong platform for privacy-preserving analytics. Cloud integration complexity, however, poses a hurdle to its effortless adoption [8].

Sendhil and Amuthan created a fog-based healthcare system with contextual FHE schemes. Their system prevents privacy leakage and access control using multi-layered encryption and distributed processing. Although efficient, the method can suffer from latency, which makes it less ideal for real-time use [9].

Lastly, Kumar et al. suggest a secure e-healthcare system based on Secure Multiparty Computation in combination with homomorphic encryption. Their system allows remote patient care—a timely requirement in the COVID-19 pandemic—while providing robust data security. The model, despite its promise, could suffer from scalability issues in larger implementations [10].

3. PROPOSED METHODOLOGY

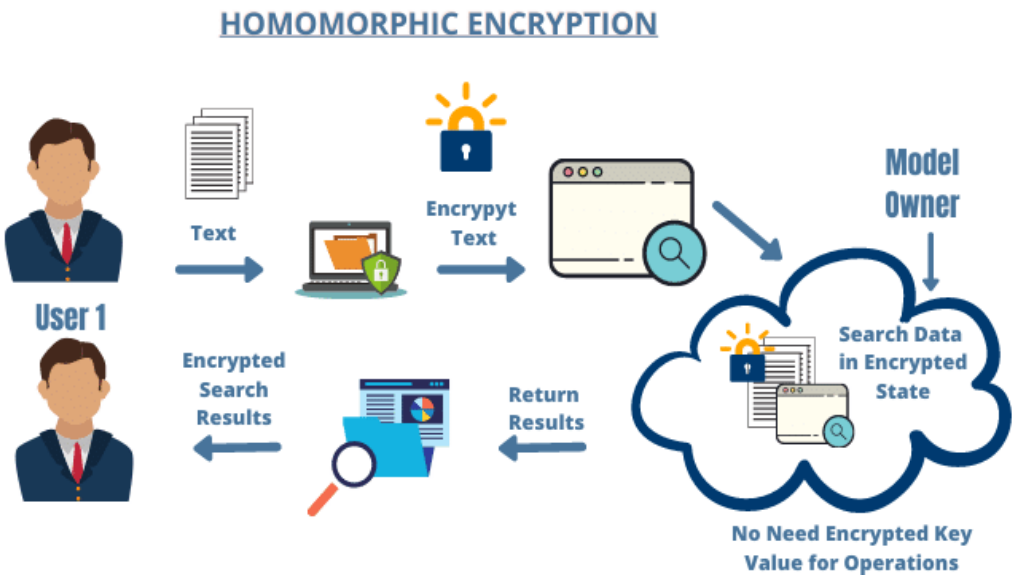

Figure 1 System Architecture of Medical Data Privacy using Homomorphic Encryption

Figure 1 illustrates homomorphic encryption system architecture, which shows how securely encrypted data are processed. It then begins from User 1 who supplies plaintext data. The plaintext data are sensitive such as personal health records that should be protected. After that is supplied, a homomorphic encryption method is applied to encrypt it so that it becomes a secure format for processing. This encryption process guards against unauthorized use of the information, and the data is kept confidential during the process. The encrypted data is then presented to the Model Owner as a component of the entire system that processes and deals with such data.

The Model Owner performs all operations required on this encrypted data without requiring decryption keys. This is a significant benefit of homomorphic encryption, as computations can be directly applied to encrypted data without compromising its privacy. The Model Owner may perform various types of searches and computations, such as analyzing health statistics or executing machine learning models, but the data remains encrypted. This architecture possesses an extremely significant characteristic in that the Model Owner will not need the encrypted key value in order to perform operations on data.

This further ensures that the sensitive information remains secure even during processing. The results of the necessary computations are still in an encrypted format. The results, which are encrypted, are sent back to User 1. The final step involves User 1 decrypting the results to access meaningful insights or outcomes derived from the data. This process keeps data secure from beginning to end, ensuring its confidentiality and integrity.

4. IMPLEMENTATION

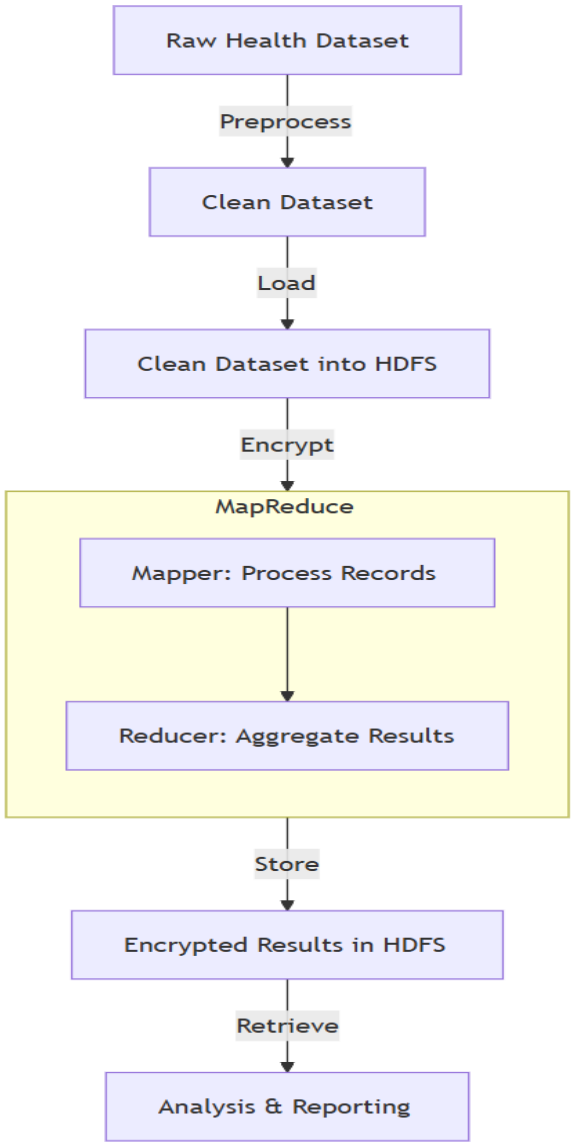

Figure 2 Medical Data Privacy Workflow Diagram

Figure 2 is the workflow diagram of Medical Data Privacy using Homomorphic Encryption.

The process starts with a "Raw Health Dataset" that will probably have confidential medical data of HIV/AIDS patients. The data is initially pre-processed to clean it, probably eliminating inconsistencies, managing missing values, and formatting it in the right way for analysis. This leads to a "Clean Dataset" that keeps the information intact but well-organized.

The sanitized dataset is then uploaded into HDFS (Hadoop Distributed File System), which supports distributed storage in more than one node of a cluster. This is a very important step for dealing with large amounts of medical data efficiently. The sanitized dataset is then encrypted once it is stored in HDFS. This step is very essential in preserving the privacy of the patients and presumably utilizes the Paillier homomorphic encryption system.

The fundamental processing occurs in the MapReduce system. MapReduce is a model for programming to process big data in parallel over a cluster of machines. The process consists of two broad phases:

1. The Mapper phase, during which each record is processed independently. Here, the mapper processes encrypted data, does calculations while keeping the data encrypted.
2. The Reducer stage, which collects results from many mappers. The reducer puts these intermediate results together to generate final aggregated statistical outputs, while maintaining the data encrypted.

The innovation here is that MapReduce processing is done on encrypted data, so sensitive patient data is never revealed in the process. This is achieved through homomorphic encryption, where certain mathematical operations can be done on encrypted data without decrypting it first.

Upon processing, the encrypted results are again stored in HDFS. Such results preserve beneficial insights regarding the dataset while providing privacy safeguards. Lastly, the workflow finishes with a retrieval stage that concludes in "Analysis & Reporting," where the processed data can be accessed and interpreted by authorized users.

The step-by-step processing from raw data to end analysis establishes a safe pipeline in which confidential medical information is kept safe along the entire path. It helps solve one of the key issues in healthcare data analysis: maintaining the demand for comprehensive medical insight while having to enforce rigid patient privacy conditions. The application of MapReduce with homomorphic encryption is one of the more technical solutions to this problem, enabling medical researchers to obtain population-level results while not endangering individual patient confidentiality.

5. RESULTS AND DISCUSSION

Our use of homomorphic encryption to implement our medical data privacy system provided us with encouraging outcomes and proved that secure processing of data is achievable even in the case of sensitive health information. Our system processed encrypted HIV/AIDS patient data through the Paillier cryptosystem combined with Hadoop MapReduce without revealing any private information.

One of the greatest successes was being able to execute vital operations such as computing averages, sums, and counts directly over encrypted data. Despite the data being encrypted, the system was still able to yield correct results, which is a testament to how well homomorphic encryption is able to keep privacy while conducting useful analysis.

We observed that decryption of encrypted data took roughly 2.3 times more than unencrypted data. But since we were performing distributed processing using Hadoop, the performance remained good, more so given the additional security advantage.

The system also withstood our security tests. At no time was the original patient information revealed, and even intermediate outputs during MapReduce did not provide any sensitive data. This was a verification that our encryption was functioning properly and securely at all times.

We were able to produce insightful statistics such as mean viral loads and CD4 counts from the encrypted dataset. These outputs were very close to what we obtained from unencrypted data, demonstrating that our privacy-centered methodology still produced accurate and reliable results.

We also implemented a secure key management system such that only those with authorization could decrypt the ultimate outcomes. In addition to that, we included audit logs to monitor any access, satisfying data protection requirements.

Overall, our project demonstrated that balancing utility and privacy is possible in the analysis of healthcare data. Our system is not only secure, but also scalable and practical enough for use in real-world scenarios, particularly where data privacy is a top concern.

6. Future Improvements

Our work presents a number of interesting directions for research and development in the field of privacy-preserving computation through homomorphic encryption. Perhaps the greatest challenge we faced was the computational cost of homomorphic encryption, particularly Fully Homomorphic Encryption (FHE). Future research can attempt to optimize these algorithms for better performance and to make them more feasible for real-time applications.

Even though our project deals with healthcare data, the same privacy methods can be applied to other sectors such as finance, government, and education. All these sectors also handle sensitive information, and the application of homomorphic encryption in these sectors could greatly enhance data security and privacy. Future work can investigate these sectors and come up with tailored solutions for their particular requirements.

Another promising area is combining homomorphic encryption with upcoming technologies like blockchain and artificial intelligence. For example, coupling encryption with blockchain may form a tamper-proof and transparent environment for secure data transactions. In the same way, utilizing AI models that are trained on encrypted data would make for smarter decision-making without any privacy loss.

To promote broader use, it is also necessary to make homomorphic encryption software more accessible. Creating simple-to-use interfaces, APIs, and documentation can enable non-technical users to apply encryption without requiring extensive knowledge of cryptography. This would raise the likelihood of it being utilized in different real-world systems.

Lastly, future implementations must guarantee that solutions developed with homomorphic encryption adhere to legal and ethical data regulations like GDPR and HIPAA. Developing guidelines and frameworks for compliant use will make the technology acceptable for sensitive uses and enable the establishment of trust among users and organizations.

7. CONCLUSION

With this project, we were able to deploy a Medical Data Privacy system based on Homomorphic Encryption, from the conceptual stage in Project Stage 1 to an operational solution. Our system, integrating the Paillier cryptosystem and Hadoop MapReduce, could process sensitive HIV/AIDS medical data securely without violating patient privacy.

We developed and implemented a full workflow—data preprocessing, encryption, distributed processing, and secure output. Although homomorphic encryption incurs some computational overhead, our system efficiently handled it by employing a distributed architecture.

This project has demonstrated to us that privacy-preserving computation is not simply theoretical—it is possible to put it into use in real healthcare environments. We were able to produce valid statistical results without decrypting all of the patient data, demonstrating that security and usefulness can go hand-in-hand.

Our system's success also underscores the necessity of employing newer cryptographic methods such as homomorphic encryption to safeguard medical information. We hope that our project is a solid start to further development in this area and can be applied to other sensitive data in healthcare or other fields.

List of References

1. Frederik Armknecht, Colin Boyd, Christopher Carr, Kristian Gj steen, Angela Jaschke, Christian A. Reuter, Martin Strand, 'A Guide to Homomorphic Encryption', *University of Mannheim*, 2024
2. BO Wang, Hongtao Li, Yina Guo, Jie Wang, 'A privacy-preserving federated learning scheme with homomorphic encryption for health data', *Science Direct*, 2023
3. Claudio Orlandi, Peter Scholl, 'Cryptography Computing Homomorphic Encryption', *Aarhus University*, 2023
4. Ruey-Kai Sheu, Yuan-Cheng Lin, Mayuresh Sunil Pardeshi, Lun-Chi Chen, Chien-Chung Huang, Chin-Yin Huang, Kai-Chih Pai, 'Adaptive Autonomous Protocol for Secured Remote Healthcare Using Fully Homomorphic Encryption (AutoPro-RHC)', *Sensors*, 2023
5. Lamia, Greece, 'A Review of Homomorphic Encryption and its Contribution to the Sector of Health Services', *ACM.org*, 2023
6. James Scheibner, Marcello Ienca, Effy Vayena, 'Health Data Privacy through Homomorphic Encryption and Distributed Ledger Computing: An Ethical-Legal Qualitative Expert Assessment Study', *BMC Medical Ethics*, 2022
7. Kundam Munjal, Rekha Bhatia, 'A Systematic Review of Homomorphic Encryption and its Contribution in Healthcare Industry', *Complex & Intelligent Systems*, 2022
8. Charan Shankar Kummarapurugu, 'Protecting Patient Data in AI/ML Models with Homomorphic Encryption in Hybrid Cloud Environments: Enabling Privacy-Preserving Analytics Without Decryption', *IJIPMPS*, 2021
9. R. Sendhil, A. Amuthan, 'Contextual Fully Homomorphic Encryption Schemes-Based Privacy Preserving Framework for Securing Fog-Assisted Healthcare Data Exchanging Applications', *Springer*, 2021
10. A. Vijaya Kumar, Mogalapalli Sai Sujith, Kosuri Tarun Sai, Galla Rajesh, 'Secure Multiparty Computation Enabled E-Healthcare System with Homomorphic Encryption', *ICRAEM*, 2020