International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 9, No. 3, 2022, pp. 31-35.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Secured Multi-Party Computations for Privacy-Preserved Medical Data Analysis

Ritika Sethi [a], Nikhil Soman [b]

[a] *Ritika Sethi, Wearable Computing Group, Chandigarh Institute of Information Technology, India.*
[b] *Nikhil Soman, Wearable Computing Group, Chandigarh Institute of Information Technology, India.*

Abstract

The "Internet + Intelligent Medical" advancement lets users detect common ailments online. The procedure for diagnosis reveals numerous significant privacy issues concerning individuals' sensitive health information. This work introduces a novel privacy-preserving self-service medical diagnosis method utilizing Secure Multi-Party Computation (SMC) to address these issues. In the protocol, a registered client first encrypts their personal health information and then transmits it to the facility's computer, which computes the similarity of the individual's medical health information and the hospital's illness trait vectors. The medical facility's server ultimately identifies the disease corresponding to the patient based on the computed similarity value. It transmits the treatment protocol for this condition to the individual in question. The self-service healthcare diagnosis system, grounded in Homomorphic Encryption (HE) and privacy-preserving access control, ensures the privacy of individual patient data and the secrecy of hospital diagnostic methods. The comprehensive security research demonstrates that the technique can withstand numerous recognized security risks. The system not only diminishes treatment costs for patients and alleviates the substantial burden on healthcare facilities during evaluation but also forecasts additional illnesses, thereby providing patients with a more transparent comprehension of how they are doing now and enabling them to receive the most suitable therapy.

Keywords: Multi Party Computations, Privacy-Preservation, Medical, Security.

DOI: 10.71086/IAJSE/V9I3/IAJSE0926
Received: 19 June 2022/Revised: 25 July 2022/Accepted: 28 August 2022/Published: 30 September 2022

Introduction

Integrating Internet connectivity with intelligent features in the "Internet + Intelligent Medical" architecture effectively addresses the challenges of accessing medical care and has demonstrated significant potential in lowering healthcare costs (Laxminarayan et al., 2016). Innovative wearable technologies are experiencing rapid growth and widespread utilization in recent years (Ometov et al., 2021). Patients can effortlessly obtain medical health information through equipment such as blood pressure meters, pacemakers, temperature sensors, respiratory monitors, endoscopic capsules, and intelligent belts. Several intelligent smartwatches offer recommendations for managing one's health, thereby conserving time for patients (Reeder & David, 2016). They provide their medical information digitally, allowing patients to perform medical inquiries and diagnoses via "Internet + Smart Medical."

The self-service medical evaluation paradigm mandates that a healthcare provider, specifically the hospital, is accountable for gathering an extensive history of clinical diagnostic information (Darzentas & Petrie, 2018). The health service company can train a diagnosis model from the acquired data using machine learning techniques. This algorithm can identify and forecast the infection status of healthcare users regarding a particular ailment. According to this approach, rural inhabitants can get expert medicine from home by utilizing their cell phones to input medical data and receive diagnostic results.

Indeed, this medical data includes sensitive patient data like arterial pressure and heartbeat (Al-Issa et al., 2019). The unforeseen leakage of health information inflicts considerable psychological distress on patients or even jeopardizes their lives, posing a primary impediment to online self-service diagnosis. For instance, Patient Home Tracking, an American business offering home health care, experienced a 48.6G data breach resulting from a cloud setup error, compromising the medical records of 160,000 individuals across the US (Joshi & Mohapatra, 2019). Criminals exploit these exposed data for lucrative transactions or to incite social unrest. People are increasingly concerned about the potential leaking of their personal health information during online medical diagnoses, which could significantly impede progress in medical diagnosis. The assessment of patient's health through privacy-preserving methods will emerge as a focal point for future studies in the healthcare domain.

Background

In wireless medical data networks, symmetric key encryption systems are more appropriate than cryptosystems with public keys for establishing secure healthcare systems due to the prevalence of numerous low-power and low-cost devices. In the past few years, various healthcare systems utilizing symmetric key encryption systems in wireless medical sensors have been presented. A study demonstrated a biometric-based decentralized key administration method for mobile body area networks (Donald, 2019). Four confidential keys are exchanged between a sensor node and the healthcare databases. The study presented a real-time, safe, wireless health surveillance system. Their recent idea employs ZigBee technology, facilitating low-power and dependable transfer of information.

The study presented a secure wellness tracking system utilizing medical wireless sensor networks. The proposed plan employs Telos-B online, facilitating low-power and dependable data transfer. The technique employs stream encryption and a code that authenticates messages to provide privacy, authentication, and integrity.

The paper presented a practical approach for privacy-preserving wireless healthcare sensor networks with an asymmetrical key cryptosystem founded on the SHA-3 hash algorithm. A lightweight encryption technique based on SHA-3 is proposed for wirelessly medical networks of sensors to secure interactions among sensor nodes and servers. To safeguard the privacy of patient information kept on computers, they divide the data into three components, the sum of which equals the initial information. Utilizing the Sharemind System (SS) provides their strategy with an additional benefit (Xia et al., 2021). The SS platform allows programmers without expertise in secure computational theory to design safe and privacy-preserving mechanisms. The number of computational players constrains the SS architecture. The present iteration of the SS architecture relies on three nodes for mining (i.e., data servers), necessitating precisely three patient-data libraries for its application in healthcare systems. In their method, every patient's information is divided into precisely three segments and saved in one of all three systems. If a healthcare facility or facility has fewer than three computer subjects, the SS platform will not benefit them.

Proposed Privacy-Preserving Machine Learning (PPML)

The PPML task involves safeguarding the confidentiality of everyone involved in the machine learning structure, wherein individuals supplying the training data during the algorithm's training period or the test data during the inference phase (referred to as customers) interact online with the model’s proprietor, who conducts calculations via

this model (designated as the server and). Simultaneously, clients need assurance regarding the confidentiality of their information (training specimens, model inquiries, and corresponding answers) from one another and their model proprietor using Secure Multi-Party Computation (SMC). The device's owner seeks to maintain customer confidentiality of its characteristics.

The circumstances in which a curiosity like this emerges vary, for instance, during processing private information and data about medical, tax, or banking confidentiality. The algorithm's owner's interests emerge when offering paid features such as pattern look, recognition of faces, processing of images, suggestions, and approaches utilizing the model. Shortly, collections of similar features evolve into venues for diverse customized offerings.

Privacy generally encompasses elements such as privacy, control over access, secrecy, non-connectivity of activities or events, indistinguishable of the event initiator, and contingent upon the unique context. Contemporary technologies and instruments offer numerous methods to get more details about an individual than she wishes: data collection breaches, retrieval of information through indirect means, data analysis (the discernment of nuanced and concealed trends within data), among others. Privacy denotes safeguarding against an excessively inquisitive opponent in its most expansive definition.

The setup for executing PPML can be illustrated by the architectural framework shown in Fig. 1.

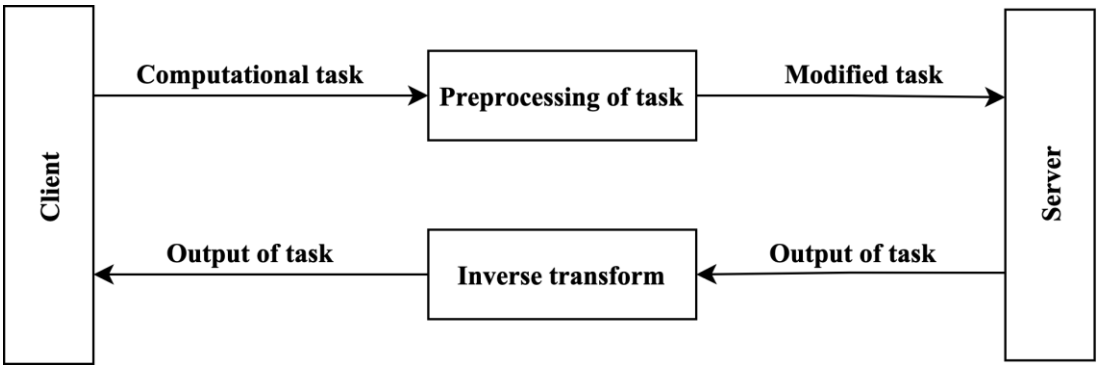


Fig. 1: PPML Architecture

Refer to the notion of secure multi-party calculations. A multi-party cryptography protocol is considered, wherein each participant possesses a distinct key. It is essential to assess the function of this private information, ensuring that the outcome of the computations is accessible to all team members. At the same time, the secrets remain undisclosed among the protocol participants and to any external parties. Let those parts of the cryptographic procedure possess private input information, respectively. Consequent to the implementation of the SMC method, they must collaboratively compute a function of the form when the criteria specified are satisfied:

Accuracy: every single person.

Privacy: no supplementary information is revealed to any individuals or external parties except what was already known before the execution of the procedure, including the interim findings of computations.

Four primary algorithmic methods exist for the implementation.

- Distorted circuits
- Confidential sharing protocols
- Homomorphic cryptography
- Zero-knowledge arguments (in certain instances for task result validation).

Results

This section employs an empirical study to validate the accuracy of the SMC self-service healthcare diagnosis framework. To simplify, the research utilizes the trait vectors from the clients' physical health information to align with the five illness trait matrices in the hospital's disease registry.

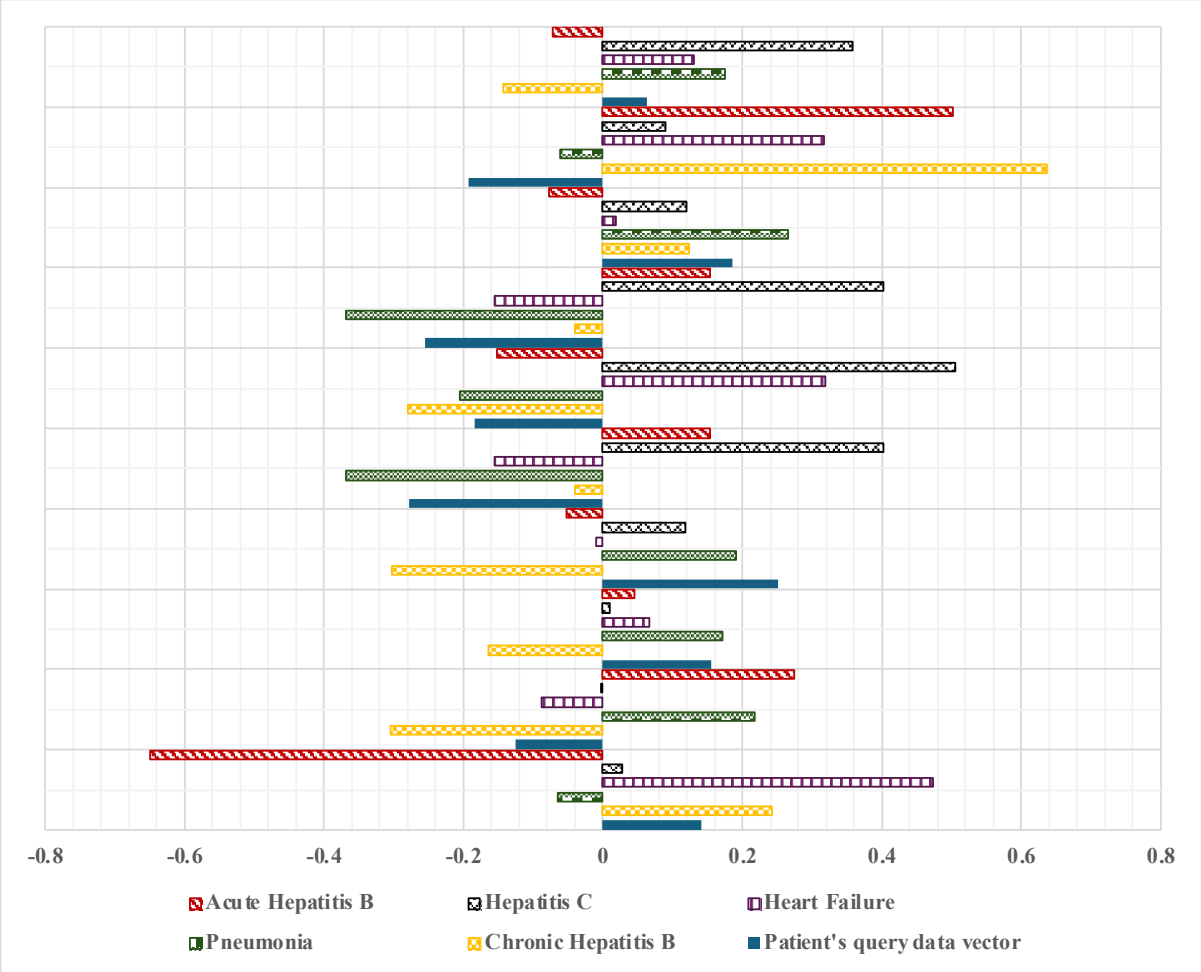


Fig. 2: Similarity Analysis

Initially, the research employed the principle component analysis to ascertain that the dimension of the patient's health-related trait vectors and the disease characteristic vector within the hospital's disease databases is 10. Clinical signs and symptoms associated with the components in these trait vectors include a transfusion-related history, mild fever (≤ 36°C), moderate to severe temperature (> 36°C), shivering, ankle swelling, anterior edema, lower limb swelling, unilateral upper-limb edema, icteric sclera, and xanthochromia. The disease information can be transformed into the trait vector form presented in Fig. 2 following processing steps, including filtering and normalizing. The illness trait vectors are essential factors for hospital diagnostics. The patient employs their medical wellness trait field to compare it with the five illness trait matrices in the hospital's disease databases, identifying the illness vector most closely aligning with their medical information trait vector. To minimize the spatial dimensions, this part utilizes only five illnesses from the hospital's illness database: respiratory infections, chronic liver disease B, coronary artery disease, liver disease, and acute liver disease.

The SMC findings indicate that the patient is likely afflicted with pneumonia, aligning with the selection of patients with pneumonia. Based on the established limit, the individual is anticipated to have mild coronary artery disease, which aligns with the severe clinical bronchitis that induces heart failure.

In the study, an individual's trait vector comprises 10 dimensions, with five illnesses in the hospital dataset. The execution duration of the plaintext calculation on the individual's side is 10 ms. Assuming there are N illnesses in the hospital's illness file, the runtime for plaintext calculation and the acquisition of the outcome is 2N milliseconds. It can facilitate a pragmatic use in medicine that diminishes the cost of diagnosis for individuals and alleviates the substantial burden on hospitals. The suggested SMC strategy is viable and highly practical, providing an alternative viewpoint for future medical diagnostics.

Conclusion

SMC self-service healthcare diagnosis presents the advantageous potential for medical assessment utilizing patients' confidential health data vectors while safeguarding patient confidentiality information. The volume of concurrent requests constrains the current methodologies for this type of medical evaluation and depends on trusted third parties, resulting in significant scalability challenges in real implementations. This work proposes a secure, self-service medical evaluation scheme based on SMC. By fully utilizing the attributes, the research has empowered a health data owner to safely transmit the majority of self-service medical evaluation operations to healthcare facilities, ensuring the scheme's achievement even with a significant disease file and a considerable volume of simultaneous requests. The method of diagnosis employs similarities in illness to measure patient conditions, leveraging all resources combined by "Internet + Smart Medical" to attain more precise diagnoses. The security assessment demonstrates that the suggested SMC scheme meets safety goals. An actual study has shown that the proposed approach is viable and possesses practical value. The suggested SMC medical evaluation system can facilitate patients in obtaining more precise therapy for their present medical conditions while alleviating the significant burden on hospitals. The research anticipates this will provide the investigator with an alternative viewpoint on the future of the medical industry.

References

Laxminarayan, R., Matsoso, P., Pant, S., Brower, C., Røttingen, J. A., Klugman, K., & Davies, S. (2016). Access to effective antimicrobials: a worldwide challenge. *The Lancet*, *387*(10014), 168-175. https://doi.org/10.1016/S0140-6736(15)00474-2

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., ... & Lohan, E. S. (2021). A survey on wearable technology: History, state-of-the-art and current challenges. *Computer Networks*, *193*, 108074. https://doi.org/10.1016/j.comnet.2021.108074

Reeder, B., & David, A. (2016). Health at hand: A systematic review of smart watch uses for health and wellness. *Journal of biomedical informatics*, *63*, 269-276. https://doi.org/10.1016/j.jbi.2016.09.001

Darzentas, J., & Petrie, H. (2018). Patient self-service paradigms in hospital and healthcare service design settings. In *Service design and service thinking in healthcare and hospital management: Theory, concepts, practice* (pp. 447-462). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-00749-2_25

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. *Journal of healthcare engineering*, *2019*(1), 7516035. https://doi.org/10.1155/2019/7516035

Joshi, A., & Mohapatra, A. K. (2019). Authentication protocols for wireless body area network with key management approach. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(2), 219-240. https://doi.org/10.1080/09720529.2019.1582869

Donald, M. (2019). Key cognitive preconditions for the evolution of language. *Handbook of Cognitive Archaeology*, 287-295.

Xia, Z., Gu, Q., Zhou, W., Xiong, L., Weng, J., & Xiong, N. (2021). STR: Secure computation on additive shares using the share-transform-reveal strategy. *IEEE Transactions on Computers*. https://doi.org/10.1109/TC.2021.3073171