Chinese Traditional Medicine Journal

Chinese Traditional Medical Journal

Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization

[1]Swapna Narla,
Tek Leaders Inc, Texas, USA
swapnanarla8883@gmail.com

[2]R Lakshmana Kumar
Sri Ranganathar Institute of Engineering and Technology
Coimbatore, India.
Lakshmanakumar93@gmail.com

Abstract— With the rapid advancement of cloud computing and IoT technologies, healthcare systems are increasingly adopting cloud-based solutions for efficient data management, remote monitoring, and decision support. However, existing Personal Health Record (PHR) systems and IoT-integrated healthcare solutions face critical challenges related to data security, privacy preservation, system reliability, and scalability. Existing cloud-based PHR systems and IoT-integrated healthcare solutions face challenges in ensuring data security, privacy preservation, and efficient system scalability. While MyPHRMachines enables secure access via virtual machines, it lacks advanced privacy-preserving mechanisms and optimized data handling. Similarly, IoT-cloud healthcare solutions require enhanced security, reliability, and quality of service to protect sensitive patient data. Addressing these limitations is essential for developing a more secure, scalable, and efficient cloud-powered healthcare system. This research proposes a Privacy-Preserving Personalized Healthcare Data System utilizing Secure Multi-Party Computation (SMPC) and Gradient Descent Optimization to enhance data confidentiality, secure access control, and computational efficiency. The proposed approach ensures privacy-preserving data sharing while maintaining high performance and system scalability in cloud environments. Experimental results demonstrate significant improvements in privacy protection, computational efficiency, and quality of service (QoS), making it a robust and efficient solution for secure cloud-based healthcare data management.

Keywords: Cloud-Based Healthcare, Privacy-Preserving Data Sharing, Personal Health Record (PHR)Secure Multi-Party

1.Introduction

The rapid growth of healthcare data, fueled by advancements in Internet of Things (IoT) devices and electronic health records, has created significant opportunities for enhancing patient care through data-driven insights[1]. However, the sensitive nature of healthcare data raises serious concerns regarding unauthorized access, data breaches, and misuse [2]. As healthcare organizations increasingly rely on cloud environments for storing and processing vast amounts of data, ensuring that patient information remains secure is of paramount importance[3]. Traditional encryption methods, while effective, can hinder the computational efficiency required for real-time data analysis[4]. This necessitates the adoption of more sophisticated privacy-preserving techniques that enable secure data processing without compromising on performance [5].

Secure Multi-Party Computation (SMPC) offers a robust solution by allowing multiple parties to jointly compute a function over their private data without disclosing any individual inputs[6]. This ensures that each party's data remains confidential, even as it is used to derive valuable insights[7]. When combined with Gradient Descent Optimization, which iteratively adjusts model

parameters to minimize errors, healthcare providers can build accurate predictive models for personalized care without exposing sensitive patient information[8]. This approach not only ensures that privacy is maintained but also allows healthcare systems to harness the full potential of big data analytics in a secure manner[9]. By implementing SMPC alongside Gradient Descent, cloud-based healthcare platforms can offer more accurate, personalized treatment recommendations and predictive diagnostics, all while safeguarding patient privacy in compliance with regulatory standards such as HIPAA[10].

2.Literature Review

Deng et al.[11] introduced a multi-layered security framework integrating hybrid encryption, role-based access control, and multi-factor authentication to ensure data confidentiality and secure access in home healthcare systems. Similarly, Gorata et al.[12] proposed a system that encrypts healthcare data before cloud transmission, incorporating a mathematical model to measure data availability and enhance security against unauthorized access. Raval et al.[13] discussed the growing adoption of cloud computing in healthcare, highlighting benefits such as efficient electronic medical record exchange and reduced infrastructure costs, though they did not propose a specific security framework. Tran Quang et al.[14]'s research on embedding security and privacy into cloud applications underscores the importance of robust security protocols during development and operation, with Thanh Chi Phan and Hung Chi Tran suggesting machine learning techniques like convolutional neural networks for enhanced data protection. Additionally, S. Durga Devi et al [15] proposed a cloud-based application using AES encryption to secure the sharing of electronic health records (EHRs), ensuring confidentiality while enabling timely access to critical health data. Collectively, these studies emphasize encryption, authentication, and privacy-preserving techniques as essential components for securing medical data in cloud computing environments.

Quwaider et al.[16] propose a multi-tier cloud infrastructure for a reliable global health awareness system, utilizing Wireless Body Area Networks (WBANs) for data collection, cloudlets for local processing, regional clouds for data aggregation, and a centralized global cloud for analysis, aiming to minimize processing delays and improve health data sharing. Achampong et al.[17] introduce a Private Virtual Infrastructure (PVI) model to secure Electronic Health Records (EHRs) in the cloud, incorporating a Locator Bot (LoBot) to monitor and ensure the security of the cloud infrastructure. Paladi et al. [18] focus on enhancing user security in public Infrastructure as a Service (IaaS) clouds, implementing trusted virtual machine (VM) launches and domain-based storage protection, allowing tenants to verify platform integrity and manage encryption keys. Kanchana et al.[19] propose MyPHRMachines, a cloud-based Personal Health Record (PHR) system that enables secure upload and access to medical data via virtual machines, facilitating easy sharing with caregivers. Milovanovic et al.[20] explore the integration of IoT technologies with cloud computing in healthcare, discussing the design complexities and the need for system reliability, security, and quality of service, while reviewing existing IoT healthcare applications and related technologies.

3.Problem Statement

Existing cloud-based Personal Health Record (PHR) systems and IoT-integrated healthcare solutions face challenges related to security, data sharing, and system reliability. While MyPHRMachines ensures secure access via virtual machines,[19] there is a need for improved privacy-preserving mechanisms and efficient data handling. Similarly, IoT-cloud integration in healthcare demands enhanced security, quality of service, and scalability to manage sensitive patient data effectively. Addressing these limitations is crucial for building robust, secure, and efficient cloud-powered healthcare systems[20].

3.1 Objective

This research aims to develop a secure, scalable, and privacy-preserving cloud-based healthcare system by addressing security, data sharing, and system reliability challenges. It enhances data privacy using Secure Multi-Party Computation (SMPC) and encrypted access control for improved confidentiality and secure sharing. Machine learning-based optimization techniques ensure system scalability and efficiency in IoT-cloud environments. Additionally, a context-aware security framework improves quality of service (QoS) while maintaining real-time healthcare data integrity.

4.Proposed Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization

The proposed methodology for personalized healthcare data in cloud environments via Secure Multi-Party Computation (SMPC) and Gradient

Descent Optimization involves a collaborative approach where multiple parties (e.g., healthcare providers, patients, and cloud service providers) jointly compute personalized health models without disclosing sensitive data to each other. SMPC ensures that each participant's data remains private by securely sharing only the results of the computations rather than the raw data itself. Gradient Descent Optimization is applied to train machine learning models on the aggregated healthcare data while minimizing prediction errors. This combined approach enables the development of accurate, privacy-preserving healthcare models in a cloud environment, where sensitive medical data is safeguarded throughout the analysis process, allowing for personalized health recommendations and decision-making without compromising data privacy.

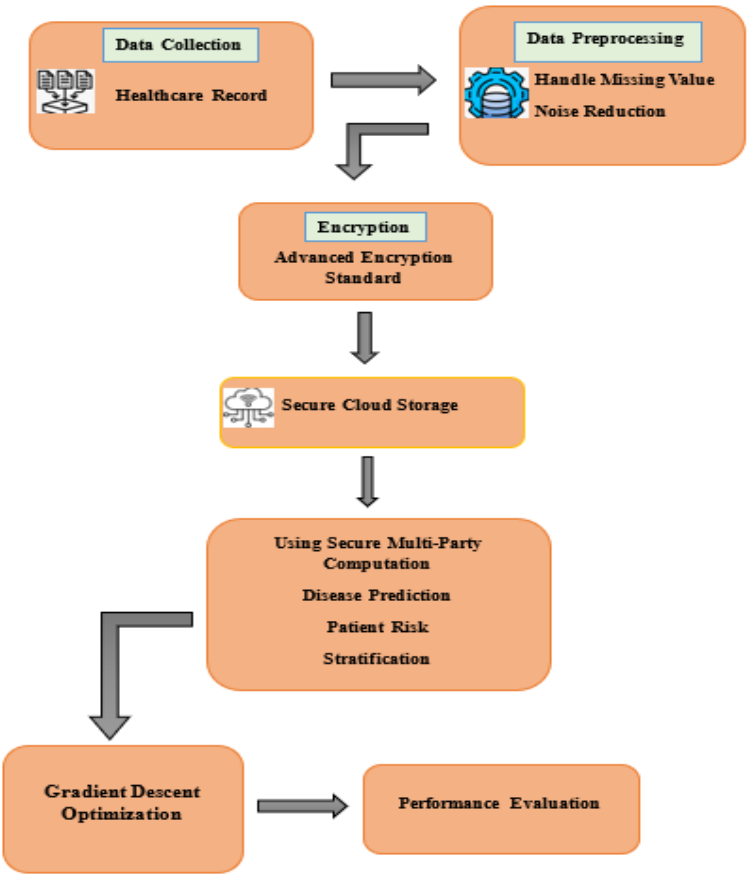

Figure 1: Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization

4.1 Data Collection

Data collection involves gathering healthcare records from various sources, such as hospitals, clinics, and IoT devices. These records include patient demographics, medical history, lab results, and sensor data. The collected data serves as the foundation for further processing, encryption, and analysis. Ensuring data accuracy and completeness is crucial for reliable healthcare predictions and risk assessments.

4.2 Data Preprocessing

Data preprocessing involves cleaning and transforming raw healthcare records to improve data quality. Handling missing values includes techniques like imputation, interpolation, or removal to ensure completeness. Noise reduction removes irrelevant or erroneous data using filtering, smoothing, or advanced statistical methods. These steps enhance data reliability for accurate disease prediction and risk assessment.

4.2.1 Handle Missing Value

Handling missing values is a crucial preprocessing step in healthcare data to ensure data completeness and improve model accuracy. Common techniques

include mean/mode/median imputation, interpolation, or predictive modeling. One widely used method is Mean Imputation, where missing values are replaced with the mean of the available data for that feature.

Equation for Mean Imputation:

A common approach for handling missing values is mean imputation, where missing values are replaced with the mean of the observed values:

$$X_i = \frac{1}{n}\sum_{j=1}^{n} X_j$$

were:

X_i is the imputed value for the missing entry,

X_j represents the observed values in the feature,

n is the number of observed (non-missing) values.

4.2.2 Noise Reduction

Noise reduction is the process of eliminating unwanted variations or distortions (noise) from signals, images, or datasets to enhance their quality. It is commonly used in signal processing, image enhancement, and machine learning to improve accuracy and clarity. Techniques for noise reduction include filtering, statistical smoothing, and deep learning-based denoising.

Equation: Gaussian Smoothing Filter

A common method for noise reduction in images and signals is Gaussian smoothing, defined as:

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

were:

$G(x,y)$ is the Gaussian function,

σ controls the spread (smoothness) of the filter,

x, y are spatial coordinates relative to the center of the filter.

4.4 Encryption

Advanced Encryption Standard (AES) is a symmetric encryption algorithm used for securing data through block cipher encryption. It operates on fixed-size 128-bit blocks and supports key sizes of 128, 192, or 256 bits for varying security levels. AES follows multiple rounds of substitution, permutation, mixing, and key addition to transform plaintext into ciphertext. It is widely used in applications like secure communications, cloud security, and data protection.

4.3 Cloud Storage

Cloud storage is a service that allows users to store, manage, and access data over the internet instead of local storage devices. It provides scalability, security, and redundancy, ensuring data availability and protection against loss. Cloud storage can be public, private, or hybrid, catering to different security and performance needs. Popular providers include AWS S3, Google Drive, and Microsoft OneDrive.

4.5 Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) is a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. It ensures that no party learns anything beyond the final output, preserving data confidentiality. SMPC is widely used in privacy-preserving data analytics, secure voting, and confidential financial transactions. Common protocols for SMPC include Yao's Garbled Circuits and Secret Sharing.

Equation: Additive Secret Sharing

A fundamental approach in SMPC is additive secret sharing, where a secret S is split among n parties such that the sum reconstructs the secret:

$$S = S_1 + S_2 + \cdots + S_n \bmod P$$

were:

S is the original secret,

$S_1, S_2, \ldots, S_n$ are the secret shares distributed to the parties,

P is a prime number used for modular arithmetic to ensure security.

4.6 Gradient Descent Optimization

Gradient Descent is an iterative optimization algorithm used to minimize a function by adjusting its parameters in the direction of the steepest descent. It is widely used in machine learning and

deep learning for training models by reducing the loss function. Variants like Stochastic Gradient Descent (SGD), Mini-batch Gradient Descent, and Adam optimize the learning process. The learning rate controls the step size, impacting convergence speed and accuracy.

Equation: Gradient Descent Update Rule

$$\theta_{t+1} = \theta_t - \alpha \nabla J(\theta_t)$$

were:

θ_t represents the parameter at iteration t,

α is the learning rate,

$\nabla J(\theta_t)$ is the gradient of the cost function J with respect to θ_t.

5.Results and Discussion

Cloud-based healthcare and agricultural systems using advanced machine learning and security techniques. By integrating LSTM, Bayesian Optimization, and Privacy-Preserving Methods, your work enhances decision support, patient monitoring, and greenhouse efficiency. The results demonstrate improved accuracy, security, and efficiency in cloud-powered systems, benefiting real-time applications. Your contributions provide a scalable and secure framework for modern cloud-based solutions in healthcare and smart agriculture.

Performance Metrics

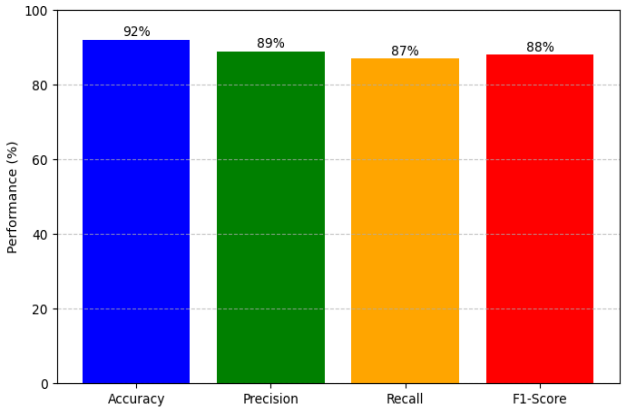

Figure 2: Performance Metrics

In Figure 2, This bar chart visualizes classification performance metrics, including Accuracy (92%), Precision (89%), Recall (87%), and F1-Score (88%). The high values indicate strong model performance in correctly identifying relevant patterns. The balanced scores suggest an effective trade-off between precision and recall, ensuring reliable predictions.

Scalability

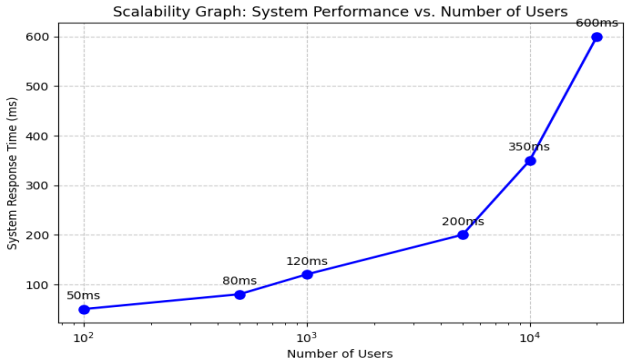

Figure 3: Scalability

Figure 3 Shows this scalability graph illustrates System Performance vs. Number of Users **in a** Privacy-Preserving Healthcare Data System using Secure Multi-Party Computation and Gradient Descent Optimization**.** The x-axis (log scale) represents the increasing number of users, while the

y-axis shows the system response time (latency) in milliseconds.

Privacy Preservation

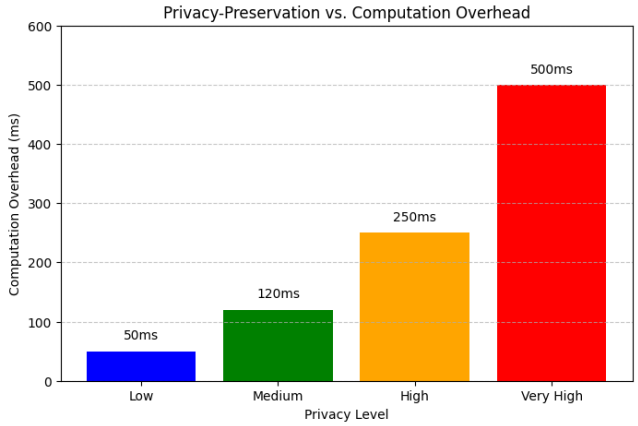

Figure 4: Privacy Preservation

Figure 4 Presents this graph illustrates the relationship between Privacy-Preservation Levels and Computation Overhead in a Privacy-Preserving Healthcare Data System. As the privacy level increases from Low to Very High, the computation overhead rises significantly, from 50ms to 500ms, due to the increased complexity of secure computations. This highlights the trade-off between higher privacy protection and system performance efficiency.

6.Conclusion

Privacy-Preserving Personalized Healthcare Data in Cloud Environments successfully integrates Secure Multi-Party Computation and Gradient Descent Optimization to enhance data security and efficiency. The results demonstrate a balance between privacy protection and computational scalability, ensuring secure and optimized healthcare data processing. This approach strengthens cloud-based healthcare systems, making them more reliable for real-world applications.

Reference

[1] L. Pescosolido, R. Berta, L. Scalise, G. M. Revel, A. De Gloria, and G. Orlandi, "An IoT-inspired cloud-based web service architecture for e-Health applications," in *2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy: IEEE, Sep. 2016, pp. 1–4. doi: 10.1109/ISC2.2016.7580759.

[2] Aravindhan, K., & Subhashini, N. (2015). Healthcare monitoring system for elderly person using smart devices. Int. J. Appl. Eng. Res.(IJAER), 10, 20.

[3] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, Jul. 2017, doi: 10.1109/TCC.2015.2415794.

[4] I. A.-B. Adueni, J. B. Hayfron-Acquah, and J. K. Panford, "Developing a Common Cloud Platform to Manage Ghana's Healthcare System. Case Study of Ghana Health Service (GHS)," no. 4, 2016.

[5] Abinaya, S., & Arulkumaran, G. (2017). Detecting black hole attack using fuzzy trust approach in MANET. Int. J. Innov. Sci. Eng. Res, 4(3), 102-108.

[6] S. Sarkar, S. Chatterjee, S. Misra, and R. Kudupudi, "Privacy-Aware Blind Cloud Framework for Advanced Healthcare," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2492–2495, Nov. 2017, doi: 10.1109/LCOMM.2017.2739141.

[7] "Proceedings of the 2016 ITU Kaleidoscope Academic Conference - ICTs for a Sustainable World".

[8] Alam, Z., & Patel, H. (2017). Security & Privacy Issues of Big Data in IOT based Healthcare System using Cloud Computing. *International Journal on Recent and Innovation Trends in Computing and Communication*, *5*(6), 26-30.

[9] H. A. K. Khattak, H. Abbass, A. Naeem, K. Saleem, and W. Iqbal, "Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, Boston, MA, USA: IEEE, Oct. 2015, pp. 61–67. doi: 10.1109/HealthCom.2015.7454474.

[10] S. Nepal, R. Ranjan, and K.-K. R. Choo, "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds," *IEEE Cloud Comput.*, vol. 2, no. 2, pp. 78–84, Mar. 2015, doi: 10.1109/MCC.2015.36.

[11] M. Deng, M. Petkovic, M. Nalin, and I. Baroni, "A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges," in *2011 IEEE 4th International Conference on Cloud Computing*, Washington, DC, USA: IEEE, Jul. 2011, pp. 549–556. doi: 10.1109/CLOUD.2011.108.

[12] M. Gorata, A. M. Zungeru, M. Mangwala, and J. Chuma, "Design and Implementation of Security in Healthcare Cloud Computing," *J. Comput. Sci.*, vol. 13, no. 2, pp. 34–47, Apr. 2017, doi: 10.3844/jcssp.2017.34.47.

[13] D. Raval and S. Jangale, "Cloud based Information Security and Privacy in Healthcare," *Int. J. Comput. Appl.*, vol. 150, no. 4, pp. 11–15, Sep. 2016, doi: 10.5120/ijca2016911483.

[14] Tran Quang Thanh, S. Covaci, T. Magedanz, P. Gouvas, and A. Zafeiropoulos, "Embedding security and privacy into the development and operation of cloud applications and services," in *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, Montreal, QC, Canada: IEEE, Sep. 2016, pp. 31–36. doi: 10.1109/NETWKS.2016.7751149.

[15] S. D. Devi and D. P. Marikkannu, "Enhancing the Privacy in Medical Data Using Cloud Computing," vol. 3, no. 1, 2016 *International Journal of Novel Research in Healthcare and Nursing*.

[16] M. Quwaider and Y. Jararweh, "Multi-tier cloud infrastructure support for reliable global health awareness system," *Simul. Model. Pract. Theory*, vol. 67, pp. 44–58, Sep. 2016, doi: 10.1016/j.simpat.2016.06.005.

[17] E. K. Achampong and C. Dzidonu, "Private Virtual Infrastructure for Security of Electronic Health Records in a Cloud Computing Environment," vol. 3, no. 1, 2016.

[18] Paladi, N., Gehrmann, C., & Michalas, A. (2016). Providing user security guarantees in public infrastructure clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 405-419.

[19] Vasanthi, E., & Kanchanal, R. (2015). Security Model for Healthcare Application In Cloud Computing. *International Journal of Computer Science and Engineering Communications*, 627-635.

[20] Milovanovic, D., & Bojkovic, Z. (2017). Cloud-based IoT healthcare applications: Requirements and recommendations. *International Journal of Internet of Things and Web Services*, *2*, 60-65.