International Journal of Mathematics, Statistics, and Computer Science
Vol. 3
ISSN: 2704-1077 eISSN 2704-1069, DOI: 10.59543/ijmscs.v3i.15181

Privacy-Preserving Integration of GPT-4 and Natural Language Processing via Secure Multi-Party Computation for Healthcare Data

Zainab Khalid Mohammed[1], Mazin Abed Mohammed [2,3*], Mohd Khanapi Abd Ghani[4] , Salah A. Aliesawi [2], Narjes Benameur[5], Korhan Cengiz[6], and Abdullah Lakhan[7]

[1]Engineering of Communication and Information Technology, Ministry of Water Resources, Baghdad, Iraq; zainabkhmohammed@gmail.com
2 Department of Artificial Intelligence, College of Computer Science and Information Technology, University of Anbar, Anbar, 31001, Iraq; mazinalshujeary@uoanbar.edu.iq ; salah_eng1996@uoanbar.edu.iq
3 Department of Cybernetics and Biomedical Engineering, VSB-Technical University of Ostrava, 70800 Ostrava, Czech Republic;
4 Department of Software Engineering, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia; khanapi@utem.edu.my
5 Laboratory of Biophysics and Medical Technologies, Higher Institute of Medical Technologies of Tunis, University of Tunis El Manar, Tunis, Tunisia; narjes.benameur@istmt.utm.tn
6 Faculty of Organization and Informatics, University of Zagreb, Croatia; kcengiz@foi.hr
7 Department of Cybersecurity and Computer Science, Dawood University of Engineering and Technology, Karachi City 74800, Sindh, Pakistan; abdullah.lakhan@duet.edu.pk

Received 10.05.2025, Revised 06.07.2025, Accepted 12.07.2025

ABSTRACT: Integrating Generative Pre-Trained Transformer (GPT-4) in healthcare heralds a transformative era, automating routine tasks and empowering physicians to focus on complex patient care. GPT-4's role in patient education simplifies medical terminology, fosters a knowledgeable patient base, and promotes adherence to care plans. This study presents a secure framework for integrating GPT-4, Natural Language Processing (NLP), and patient data in healthcare using Secure Multi-Party Computation (MPC). The framework ensures secure data exchange among stakeholders in healthcare data analysis. Emphasizing security, privacy, and regulatory compliance, the study underscores collaboration with privacy, security, and healthcare experts. The amalgamation of GPT-4 and NLP advances research and care and upholds data protection standards. The revolutionary use of MPC marks a paradigm shift, promising enhanced patient outcomes and securing the future of healthcare.

Keywords: Artificial Intelligence, Healthcare, GPT-4, Natural Language Processing, Secure Multi-Party Computation.

1. INTRODUCTION

The Generative Pretrained Transformer (GPT) paradigm, exemplified by OpenAI's ChatGPT [1–2], is a versatile tool in Artificial Intelligence language processing with applications ranging from query resolution to content generation [3,4]. In healthcare, ChatGPT enhances patient experiences and optimizes procedural workflows [5,6]. Leveraging Machine Learning algorithms and natural language processing, it excels in applications like chatbots, customer service, and digital assistants [5,6]. Despite its proficiency in honest conversations and continuous learning from identifiable patient data [7,8,9], careful adjustment is necessary for its ethical deployment in mental health tasks [9,12,13]. The tools role in customer data analysis supports customer segmentation and targeted marketing campaigns [14–15]. Demonstrating high accuracy in various dialogues [10–11], meticulous fine-tuning is essential for specific applications [9].

ChatGPT's natural language comprehension proficiency in healthcare is a critical focal point [9,16,17]. Its potential to enhance treatment adherence, deliver practical care, and improve patient outcomes, especially in underserved areas, is noteworthy [18,19]. Despite concerns about prediction capabilities and potential hallucinations in medical contexts, ChatGPT serves as a valuable resource for individuals facing challenges in accessing healthcare professionals due to geographical barriers [20,21]. In the realm of healthcare, the evolution of Artificial Intelligence (AI) technologies, exemplified by GPT-4, is Reshaping patient-physician interactions [24]. ChatGPT, a resource for individuals navigating diabetes diagnoses, improves disease management, and fosters stakeholder communication [9,22,23]. GPT-4's advanced language model anticipates a paradigm shift with nuanced understanding, heightened context awareness, and reduced biases. Particularly noteworthy attributes include improved multilingual support and superior inference of implicit user queries. In gastroenterology, effective communication is critical, and GPT-4 emerges as an innovation to enhance this interaction, reflecting current advancements and offering a promising outlook for medical consultations in this specialty [24].

This study focuses on the privacy-preserving integration of GPT-4 and NLP through Secure Mul-ti-Party Computation (MPC), aiming to establish a secure framework for collaboration while prioritizing confidentiality and privacy in healthcare data. The research assesses the efficiency and effectiveness of this integration method, evaluating its applicability and benefits in the healthcare domain. Contributions of this study include:

- Enhanced Privacy in Healthcare Data Integration: Introduces a privacy-preserving method for integrating GPT-4 and NLP in healthcare, emphasizing confidentiality, regulatory compliance (such as HIPAA), and the protection of patient information.
- Advanced GPT-4 and NLP Integration in Healthcare: Pioneers seamless integration of GPT-4 and NLP in healthcare, optimizing collaboration and improving language processing.
- Secure Health Information Exchange Facilitation: Establishes a secure framework for healthcare infor-mation exchange utilizing Secure MPC. Minimizes unauthorized access risks and ensures compliance with data protection regulations.

The structure of this paper unfolds in the following manner: Section 2 furnishes an overview of related work. Section 3 delineates the Proposed Framework, presenting the novel approach developed for the study. Moving forward, Section 4 delves into the results and discussion, offering a comprehensive analysis of the findings. Section 5 is dedicated to the evaluation and validation processes employed in scrutinizing the proposed framework. Section 6 provides the advantages of the proposed framework within the healthcare context. Section 7 deliberates on the managerial implications of implementing the proposed framework. Subsequently, Section 8 outlines the limitations inherent in the proposed framework, providing a nuanced understanding of its constraints. Finally, Section 9 encapsulates the research with a conclusion, offering insights into this study's overall findings and contributions.

2. RELATED WORKS

Privacy-preserving healthcare data integration with GPT-4 and NLP involves advancements in Privacy-Preserving Machine Learning (PPML), with methodologies such as Federated Learning (FL), Differential Privacy (DP), and Secure MPC gaining traction [25,26,27]. The NLP models are crucial for processing Electronic Health Record (EHR) data [25,26,27]. While GPT-4 applications in healthcare are limited and reveal biases [28, 29,30], privacy-preserving integration benefits from FL, DP, and MPC technologies. FL faces challenges like lower accuracy and privacy concerns [31,32]. DP focuses on output privacy, preventing inference from model output, while MPC safeguards input privacy. Researchers explore diverse privacy techniques, combining DP with randomized response and expectation maximization for enhanced resilience against security breaches and query attacks [34]. In the realm of privacy-preserving methods, recent studies explore gradient perturbation in differential privacy [35], a partitioning algorithm for efficient query workload management [36], and the effectiveness of differential privacy for extensive data privacy mechanisms [37]. Other approaches include a multi-step differential privacy classification method [38], addressing privacy concerns with a generalization lattice and deterministic disclosure function [39]. Differential privacy is recognized for its lighter computational overhead compared to Secure MPC but introduces noise affecting accuracy, while MPC ensures mathematically provable privacy protection without sacrificing accuracy [31,40]. Recent research in Privacy-Preserving Machine Learning (PPML) has utilized Secure MPC for secure inference with pre-trained models [41–42] and training various models, including linear regression [43], decision trees [44–45] and neural networks [46–47].

The importance of MPC in privacy-preserving collaborative computations is evident, reshaping secure machine learning protocols [33]. However, applying these approaches, including MPC, to integrate GPT-4 and NLP in healthcare data remains underexplored, emphasizing the need to address existing limitations and vulnerabilities. Ongoing research continues to evolve efforts to enhance the security and efficacy of privacy-preserving techniques for GPT-4 and NLP integration in healthcare [33].

This study introduces a pioneering privacy-preserving framework for integrating GPT-4 and NLP in healthcare, leveraging Secure MPC to ensure confidentiality and privacy compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The approach enhances language processing capabilities in healthcare while prioritizing a secure environment for health information exchange. The study minimizes the risk of unauthorized access by addressing the collaborative needs of multiple parties, particularly in patient care or medical research. The methodology serves as a model for ethical AI deployment in healthcare, emphasizing responsible innovation and safeguarding patient privacy.

3. THE PROPOSED FRAMEWORK

In this section, we present the methodology behind the proposed framework for integrating Generative Pretrained Transformer (GPT-4) [24] and Natural Language Processing (NLP) [25] via Secure MPC for Healthcare Data [40], depicted in Fig. 1.

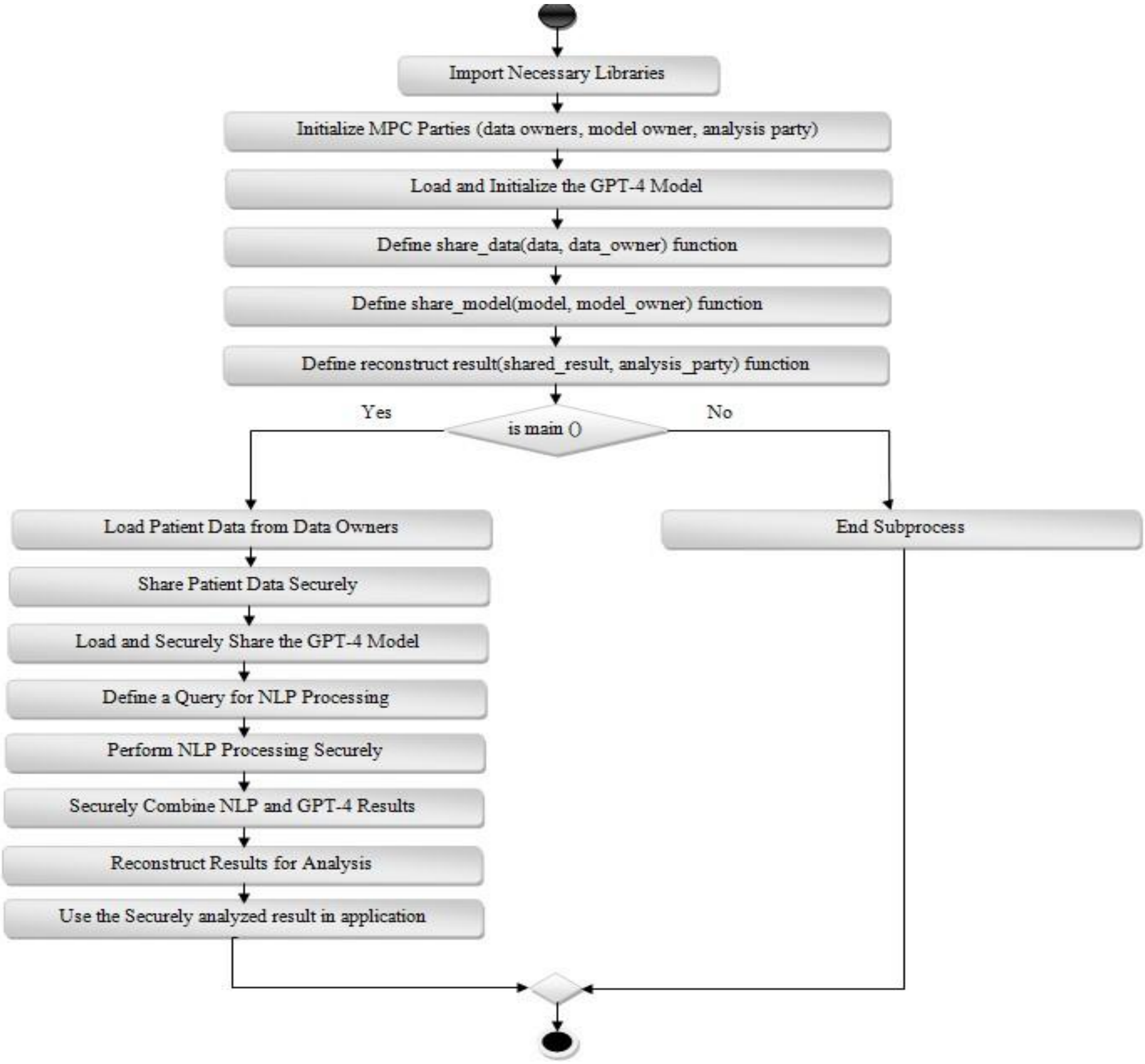
Import Necessary Libraries
Initialize MPC Parties (data owners, model owner, analysis party)
Load and Initialize the GPT-4 Model
Define share_data(data, data_owner) function
Define share_model(model, model_owner) function
Define reconstruct result(shared_result, analysis_party) function
Yes
is main ()
No
Load Patient Data from Data Owners
Share Patient Data Securely
Load and Securely Share the GPT-4 Model
Define a Query for NLP Processing
Perform NLP Processing Securely
Securely Combine NLP and GPT-4 Results
Reconstruct Results for Analysis
Use the Securely analyzed result in application
End Subprocess

Fig. 1: The Proposed Framework

The proposed framework outlines the distinct phases involved in achieving the Privacy-Preserving Integration of GPT-4 and NLP through Secure MPC for Healthcare Data:

Phase 1: Setup and Initialization

In the inaugural stage of the research framework, crucial steps are undertaken to establish the infrastructure and prepare the components essential for the secure MPC analysis of healthcare data. The process is delineated into key tasks for clarity and precision.

1. Importation of Libraries:

- Secure MPC Library: secure_mpc_library is a toolkit for secure computations, encompassing cryptographic protocols and functions.
- GPT-4 Library: gpt4 code includes functions for loading, initializing, and using the advanced GPT-4 model, known for language processing.

- NLP Library: nlp_library is imported for text analysis, parsing, and feature extraction, crucial for processing textual patient symptom data in subsequent phases.

2. Initialization of Parties:

- Data Owners: Virtual workers (data_owner_1 and data_owner_2) representing entities with patient data are initialized, ensuring secure participation.
- Model Owner: The model_owner oversees and maintains the GPT-4 model, securely sharing it for analysis while safeguarding intellectual property.
- Analysis Party: The analysis_party executes computations, amalgamates results, and extracts insights, playing a pivotal role in deriving meaningful conclusions without compromising sensitive information in the MPC process.

3. Loading and Initialization of the GPT-4 Model:

- The GPT-4 model, renowned for its proficiency in natural language understanding and generation, is load and initializ. This entails loading its parameters and configurations, placing it in a state ready for NLP tasks.
- Initialization of the model owner's virtual worker with the GPT-4 model ensures its readiness for secure and private computations in subsequent phases, preserving the confidentiality and integrity of the model's knowledge.

Phase 2: Secure Data Sharing

In the second phase of the research framework, dedicated efforts are made to establish a secure mechanism for sharing crucial components such as patient data, the GPT-4 model, and analysis results. This phase is meticulously designed to prioritize data privacy and uphold the confidentiality of sensitive information throughout the analytical process. The following elucidates the intricacies of this phase:

4. Definition of Sharing Functions:

- Secure Data Sharing Functions: Functions are crafted for securely sharing patient data, the GPT-4 model, and analysis results using the secure MPC library, incorporating cryptographic protocols for privacy.
- share_data Function: This function securely shares patient data using the MPC library, generating a shared version to prevent access to raw data.
- share_model Function: Similar to share_data, this function securely shares the GPT-4 model, preserving its parameters and intellectual property.
- Reconstruct result Function: This function finalizes analysis results, reconstructing insights for sharing while safeguarding patient data privacy.

5. Secure Data Loading:

In this step, the framework securely loads comprehensive patient data from data owners such as data_owner_1 and data_owner_2. This data includes vital information like patient names, ages, genders, and reported symptoms, forming a crucial component for subsequent healthcare analysis. The secure loading process marks the commencement of the secure MPC, ensuring the confidentiality and integrity of the patient data throughout the analytical phases.

6. Secure Data Sharing:

In this step, the framework ensures data confidentiality by employing the `share_data` function to securely share patient data with data_owner_1 and data_owner_2. This mechanism is essential for meeting the non-negotiable requirements of patient confidentiality and data protection in healthcare. It plays a critical role in preserving patient privacy, enabling meaningful analysis, and setting the foundation for subsequent phases in the secure MPC framework.

Phase 3: Secure Model Sharing

This phase focuses on the meticulous sharing of the GPT-4 model, a crucial component for natural language understanding and generation. The process ensures confidentiality and integrity by design, with the model owner (`model_owner`) being the designated recipient. The salient aspects of this phase are delineated as follows:

7. Secure Model Sharing:

In this step, the GPT-4 model, specialized in natural language processing, undergoes a secure transmission to the model owner (`model_owner`) through the Secure MPC framework, utilizing the `share_model` function from Phase 2. This process is crucial for protecting the significant investment in model development and safeguarding proprietary information, with MPC ensuring confidentiality and integrity. The securely shared GPT-4 model is then ready for tasks like processing natural language queries while maintaining a steadfast commitment to privacy and security.

Phase 4: Data Analysis and Processing

Within this phase, a meticulous approach is adopted for analyzing and processing healthcare data, integrating NLP [25] techniques. The delineation of this phase unfolds as follows:

8. Define NLP Query:

In this phase, the query "Analyze patient symptoms" is crucial for guiding subsequent NLP processing, providing clear instructions to extract relevant information from patients' symptoms. The precision in formulating the query is vital for establishing the analytical scope in healthcare contexts and directing the analysis toward predefined goals, ensuring alignment with the intended purpose.

9. Secure NLP Processing:

In this step, the defined NLP query is processed securely using Secure MPC protocols. NLP functions extract insights from patient symptoms while preserving data confidentiality. This privacy-preserving approach allows computations on shared data without disclosing information, ensuring the extraction of valuable healthcare insights without compromising patient confidentiality.

Phase 5: Integration of NLP and GPT-4 Results

Within this phase, NLP and GPT-4 results are securely integrated, aiming to synthesize insights from both processes into a coherent result, utilizing the shared GPT-4 model.

10. Secure Result Combination:

In this step, NLP and GPT-4 results are meticulously combined, focusing on data privacy utilizing secure MPC and cryptographic protocols. This ensures patient data remains confidential during integration, resulting in a comprehensive analysis that combines reported symptoms and medical context while safeguarding sensitive information.

Phase 6: Reconstruction and Analysis of Results

Within this phase, insights from NLP and the GPT-4 model are securely reconstructed to form the final result, emphasizing confidentiality and protection throughout the process.

11. Result Reconstruction:

The `reconstruct_result` function ensures secure result reconstruction through advanced techniques in secure MPC, preserving patient data confidentiality. The reconstructed result is then transferred to the analysis party, maintaining privacy and integrity. This critical step bridges secure data processing and subsequent analysis, providing valuable healthcare insights while upholding privacy principles.

Phase 7: Application of Securely Analyzed Result

The implementation of the securely analyzed result, derived from integrated patient data analysis, NLP, and GPT-4, serves healthcare by generating reports, formulating treatment plans, contributing to research, and aiding decision-making. The output, including conditions, diagnoses, and recommendations, prioritizes privacy through secure MPC, aligning with healthcare regulations and ethical standards for responsible data handling in trustful healthcare applications.

Each phase of this meticulously structured framework plays a pivotal role in contributing to the overarching objective of secure healthcare data analysis. The foremost priority throughout this process is the unwavering commitment to safeguarding patient privacy, an ethical imperative in the world of healthcare. Each phase ensures that sensitive patient data remains confidential while extracting invaluable insights crucial for medical diagnosis and treatment. The seamless orchestration of secure data sharing, meticulous processing, and the harmonious merging of data and model results is at the core of this framework. In summary, the following presented pseudocode encapsulates the foundational architecture of the proposed framework, serving as a comprehensive illustration of the Privacy-Preserving Integration of GPT-4 and NLP through Secure MPC for the secure handling of healthcare data. The Pseudo Code of the Proposed Framework's in Algorithm 1.

Algorithm1: The Pseudo Code of the Proposed Framework's

```
Phase1: Setup and Initialization
1- Importation of Libraries
import secure_mpc_library as mpc
import gpt4
import nlp_library as nlp
2. Initialization of MPC parties (data owners, model owner, analysis party)
data_owner_1 = mpc.VirtualWorker(id="DataOwner1")
data_owner_2 = mpc.VirtualWorker(id="DataOwner2")
model_owner = mpc.VirtualWorker(id="ModelOwner")
analysis_party = mpc.VirtualWorker(id="AnalysisParty")
3. Loading and Initialization of the GPT-4 Model
gpt4_model = gpt4.load_model()
```

```
Phase 2: Secure Data Sharing
4. Definition of Sharing Functions
function share_data(data, data_owner) {
    shared_data = mpc.share(data, data_owner)
    return shared_data
}
function share_model(model, model_owner) {
    shared_model = mpc.share(model, model_owner)
    return shared_model
}
function reconstruct_result(shared_result, analysis_party) {
    result = mpc.reconstruct(shared_result, analysis_party)
    return result
}
5. Secure Data Loading
if is_main():
    # Load patient data from data owners
    patient_data_1 = data_owner_1.load_patient_data()
    patient_data_2 = data_owner_2.load_patient_data()
Phase 3: Secure Model Sharing
7. Secure Model Sharing
    shared_data_1 = share_data(patient_data_1, data_owner_1)
    shared_data_2 = share_data(patient_data_2, data_owner_2)
    shared_gpt4_model = share_model(gpt4_model, model_owner)
Phase 4: Data Analysis and Processing
8. Define NLP Query
    query = "Analyze patient symptoms."
9. Secure NLP Processing
    shared_nlp_result = nlp.process_data(query, shared_data_1, shared_data_2)
Phase 5: Integration of NLP and GPT-4 Results
10. Secure Result Combination
    combined_result = gpt4.process_nlp(shared_gpt4_model, shared_nlp_result)
Phase 6: Reconstruction and Analysis of Results
11. Result Reconstruction
    analysi
s_result = reconstruct_result(combined_result, analysis_party)
Phase 7: Application of Securely Analyzed Result
12. Implementation of the Securely Analyzed Result
        process_analysis_result(analysis_result)
```

The provided pseudocode delineates a simplified conceptual representation of the Privacy-Preserving Integration of GPT-4 and NLP through Secure MPC for the secure handling of healthcare data. The pseudocode encompasses key elements, commencing with the importation of requisite libraries, including those for secure MPC, the GPT-4 model, and an NLP library. This foundational step is integral for facilitating secure computations and leveraging machine learning models. Subsequently, the pseudocode initiates the MPC by creating four virtual workers, symbolizing distinct parties involved in the computation, such as data owners, the model owner, and the analysis party. These entities engage collaboratively while safeguarding the privacy of their individual inputs. The GPT-4 model is loaded into memory, signifying a critical preparation step for secure computation. The pseudocode then defines secure sharing functions, including those for sharing data, the model, and results, utilizing the MPC library to guarantee secure information exchange without revealing the actual data or model. The main application logic unfolds in a structured manner, involving the loading of sensitive patient data, its secure sharing, loading and secure sharing of the GPT-4 model, definition of an NLP query, secure NLP processing, secure combination of NLP and GPT-4 results, secure result reconstruction, and finally, the utilization of the securely analyzed result for further applications within the healthcare domain. In summary, the pseudocode establishes a robust framework for the secure analysis of healthcare data, prioritizing privacy preservation through MPC and phased processes, thereby rendering it apt for handling sensitive medical information.

4. RESULTS AND DISCUSSION

In Section 4.1, we detail the outcomes of the Setup and Initialization Phase, while Section 4.2 explores the Secure Data Sharing Phase. Section 4.3 focuses on the Results of the Secure Model Sharing Phase, and Section 4.4 provides an in-depth analysis of the Data Analysis and Processing Phase. The Results of the combined NLP and GPT-4 Phase are discussed in Section 4.5, followed by the Reconstruction and Analysis Phase results in Section 4.6. Section 4.7 summarizes the outcomes of the Application of the Securely Analyzed Phase. The provided pseudocode was implemented in a carefully curated Python environment, ensuring compatibility and a seamless synergy between the framework's functionalities and the programming language. The meticulous selection process highlights the importance of harmonizing programming tools with the chosen language for optimal performance.

4.1 Results of Setup and Initialization Phase

1. Import Libraries:

Key libraries are imported in the Setup and Initialization Phase:

- Secure MPC Library: 'secure_mpc_library' is imported, facilitating secure MPC with cryptographic data sharing and computations protocols.
- GPT-4 Library: The 'gpt4' library is imported, enabling loading and utilization of the advanced GPT-4 language model for natural language understanding.
- NLP Library: 'nlp_library' is imported, providing tools for text analysis and feature extraction crucial for processing patient symptom data in later phases.

2. Initialize Parties:

Parties are initialized in the Secure Data Sharing Phase:

- Data Owners: Virtual workers (data_owner_1 and data_owner_2) representing entities like hospitals securely share patient data.
- Model Owner: Virtual worker (model_owner) is set up to manage and securely share the GPT-4 model, ensuring intellectual property protection.
- Analysis Party: Virtual worker (analysis_party) is created for secure computations, result combination, and insight generation through MPC.

A comprehensive dataset for 20 patients is created in Python for the proposed system. This hypothetical patient dataset includes crucial attributes like Name, Age, Gender, and Symptoms, exemplified in Table I, featuring details for the patients.

Table 1 Assumed Patients Data

Patients	**Patients Data**			
	Name	**Age**	**Gender**	**Symptoms**
Patient 1	John Doe	45	Male	Fever, Cough, Fatigue
Patient 2	Jane Smith	55	Female	Shortness of breath, Headache
Patient 3	David ohnson	35	Male	Sore throat, Runny nose
Patient 4	Emily Brown	42	Female	Nausea, Vomiting, Abdominal pain
Patient 5	Michael Wilson	60	Male	Joint pain, Muscle weakness
Patient 6	Sarah Davis	28	Female	Cough, Fatigue
Patient 7	Robert Clark	50	Male	Shortness of breath, Fever
Patient 8	Lisa Adams	70	Female	Sore throat, Runny nose
Patient 9	William White	32	Male	Nausea, Vomiting, Abdominal pain
Patient 10	Karen Brown	47	Female	Joint pain, Headache
Patient 11	Sarah Smith	38	Female	Fever, Sore throat
Patient 12	Robert Johnson	52	Male	Fatigue, Cough
Patient 13	Jennifer Lee	29	Female	Runny nose, Muscle weakness
Patient 14	Michael Brown	44	Male	Nausea, Abdominal pain
Patient 15	Emily Wilson	63	Female	Joint pain, Shortness of breath

Patient 16	David Davis	30	Male	Headache, Vomiting
Patient 17	Karen Roberts	41	Female	Cough, Shortness of breath
Patient 18	John White	57	Male	Sore throat, Fatigue
Patient 19	Lisa Harris	48	Female	Fever, Muscle weakness
Patient 20	William Clark	55	Male	Vomiting, Abdominal pain

Table 1, designated as Assumed Patients Data, presents a comprehensive dataset of 20 patients, each identified by a unique patient number, name, age, gender, and a list of associated symptoms. Serving as a fundamental resource for algorithm development and testing within a controlled environment, this dataset establishes a foundational element for subsequent phases in the system. Patient 1, exemplified by John Doe, is a 45-year-old male with symptoms of fever, cough, and fatigue, while Patients 2 through 20 display distinctive combinations of demographic information and symptoms, contributing to the dataset's comprehensive representation. This structured patient data not only facilitates the development and testing of algorithms but also provides an illustrative and controlled environment for further phases in the system, ensuring robustness and accuracy in healthcare-related computational tasks.

To further streamline data accessibility and manipulation, Table 2 A refines the patient information into Python dictionaries.

Table 2 Patient Data in a List of Dictionaries

Patient Data in a List of Dictionaries

```
patient_data = [
    {"Name": "John Doe", "Age": 45, "Gender": "Male", "Symptoms": ["Fever", "Cough", "Fatigue"]},
    {"Name": "Jane Smith", "Age": 55, "Gender": "Female", "Symptoms": ["Shortness of breath", "Headache"]},
    {"Name": "David Johnson", "Age": 35, "Gender": "Male", "Symptoms": ["Sore throat", "Runny nose"]},
    {"Name": "Emily Brown", "Age": 42, "Gender": "Female", "Symptoms": ["Nausea", "Vomiting", "Abdominal pain"]},
    {"Name": "Michael Wilson", "Age": 60, "Gender": "Male", "Symptoms": ["Joint pain", "Muscle weakness"]},
    {"Name": "Sarah Davis", "Age": 28, "Gender": "Female", "Symptoms": ["Cough", "Fatigue"]},
    {"Name": "Robert Clark", "Age": 50, "Gender": "Male", "Symptoms": ["Shortness of breath", "Fever"]},
    {"Name": "Lisa Adams", "Age": 70, "Gender": "Female", "Symptoms": ["Sore throat", "Runny nose"]},
    {"Name": "William White", "Age": 32, "Gender": "Male", "Symptoms": ["Nausea", "Vomiting", "Abdominal pain"]},
    {"Name": "Karen Brown", "Age": 47, "Gender": "Female", "Symptoms": ["Joint pain", "Headache"]}
{"Name": "Sarah Smith", "Age": 38, "Gender": "Female", "Symptoms": "Fever, Sore throat"},
    {"Name": "Robert Johnson", "Age": 52, "Gender": "Male", "Symptoms": "Fatigue, Cough"},
    {"Name": "Jennifer Lee", "Age": 29, "Gender": "Female", "Symptoms": "Runny nose, Muscle weakness"},
    {"Name": "Michael Brown", "Age": 44, "Gender": "Male", "Symptoms": "Nausea, Abdominal pain"},
    {"Name": "Emily Wilson", "Age": 63, "Gender": "Female", "Symptoms": "Joint pain, Shortness of breath"},
    {"Name": "David Davis", "Age": 30, "Gender": "Male", "Symptoms": "Headache, Vomiting"},
    {"Name": "Karen Roberts", "Age": 41, "Gender": "Female", "Symptoms": "Cough, Shortness of breath"},
    {"Name": "John White", "Age": 57, "Gender": "Male", "Symptoms": "Sore throat, Fatigue"},
    {"Name": "Lisa Harris", "Age": 48, "Gender": "Female", "Symptoms": "Fever, Muscle weakness"},
    {"Name": "William Clark", "Age": 55, "Gender": "Male", "Symptoms": "Vomiting, Abdominal pain"}
]
```

Table 2, containing Patient Data in a List of Dictionaries, exemplifies a refined approach to organizing and presenting patient information for enhanced data accessibility and manipulation. Each patient's details, including "Name," "Age," "Gender," and a list of "Symptoms," are encapsulated within a

Python dictionary, offering a structured and versatile representation of the dataset. The transition from a traditional tabular format to this dictionary-based structure optimizes data handling, providing a more intuitive framework for computational processes. The utilization of a list of dictionaries facilitates seamless integration into diverse computational frameworks, ensuring adaptability and versatility in algorithmic applications. This transformation not only supports a range of healthcare data tasks for the twenty patients but also promotes efficient and comprehensive analysis, underscoring the significance of adopting such organized data structures in advancing computational healthcare methodologies.

3. Load and Initialize Model:

The GPT-4 model [24] is loaded and initialized, establishing a secure foundation for healthcare data analysis. This phase involves library imports, secure communication channel initialization, and GPT-4 preparation, ensuring the model's integrity and patient data confidentiality for privacy-preserving insights.

4.2 Results of Secure Data Sharing Phase

The Secure Data Sharing Phase focuses on demonstrating the framework's commitment to patient data confidentiality through secure protocols. Using the `share_data` function based on secure MPC, patient data is securely shared, exemplified by encrypted shared data variables (e.g., Shared Data 1 to Shared Data 20) in Table 3. The `share_model` function underscores the importance of securing the GPT-4 model's confidentiality. This dual approach highlights the framework's comprehensive security measures, emphasizing privacy in both patient data and model information.

Table 3 Creation of Shared Data Variables with Encrypted Content

Shared Patient Data (Securely Shared with Data Owners)
Shared Data 1: [Encrypted Data]
Shared Data 2: [Encrypted Data]
Shared Data 3: [Encrypted Data]
….
Shared Data 20: [Encrypted Data]

Table 3 demonstrates a crucial aspect of the healthcare data analysis framework, featuring the creation of encrypted shared patient data variables (`Shared Data 1` to `Shared Data 20`) through secure MPC. The `share_data` function ensures secure and confidential sharing of patient data, covering names, ages, genders, and symptoms. This privacy-focused approach safeguards against unauthorized access and disclosure, essential in healthcare. The simultaneous sharing of encrypted data from various sources highlights the framework's scalability, emphasizing its commitment to data accuracy and integrity.

4.3 Results of Secure Model Sharing Phase

In Phase 3, the framework emphasizes secure GPT-4 model sharing with the model owner, ensuring confidentiality and integrity. The representation of the shared GPT-4 model as [Encrypted Model] in Table 4 underscores the unwavering commitment to privacy and security in the analysis process.

Table 4 Shared GPT-4 Model

Shared GPT-4 Model (Securely Shared with the Model Owner)
Shared GPT-4 Model: [Encrypted Model]

Table 4 visually represents the secure sharing of the GPT-4 model, denoted as [Encrypted Model], highlighting the commitment to privacy and security principles through robust encryption. The term "[Encrypted Model]" symbolizes a strong defense against unauthorized access or tampering. The secure sharing, facilitated by the `share_model` function in Phase 2, aligns with ethical considerations in healthcare data protection. It ensures the confidential and tamper-proof transmission of the GPT-4 model, reinforcing the framework's dedication to securing valuable assets in healthcare data analysis. The encrypted model maintains confidentiality and integrity for subsequent analysis phases while upholding a steadfast commitment to data protection.

4.4 Results of Data Analysis and Processing Phase

In Phase 4, Data Analysis and Processing, the healthcare data analysis framework engages in crucial activities to derive meaningful insights from the shared patient data, with a focus on secure NLP. Here's an in-depth overview of the key elements and the output:

- Define NLP Query: The phase begins with the definition of a specific NLP query: "Analyze patient symptoms." This well-defined query serves as a guiding directive for the NLP system, ensuring that the analysis aligns precisely with the intended objectives. This step is particularly important in healthcare contexts to maintain focus and relevance in the analysis.

- Secure NLP Processing: Once the NLP query is established, the code proceeds with secure NLP processing. This involves processing both the NLP query and the patient data, which was securely shared using MPC protocols introduced in earlier phases. The utilization of secure NLP processing techniques ensures that computations can be performed on shared data without revealing raw data to any party involved. This privacy-preserving approach is critical in healthcare settings where the sensitivity of patient data is paramount.
- NLP System's Role: The NLP system's role is pivotal in processing the symptoms reported by the patients. It uncovers relevant patterns, correlations, or other insights specified by the query. Importantly, this process is conducted while safeguarding data security and privacy, ensuring that patient data remains confidential and undisclosed throughout the analysis. The NLP system acts as a key player in extracting meaningful information from the patients' symptoms in a secure and privacy-preserving manner.

Table 5 NLP Processing Result

NLP Processing Result (securely processed with NLP)
Shared NLP Result: [Encrypted NLP Result]

Table 5, signifies the outcome of the NLP phase in the healthcare data analysis framework. The NLP Processing Result, securely processed with NLP techniques, is encapsulated within the variable "Shared NLP Result" and is represented as "[Encrypted NLP Result]." This result is a testament to the commitment to privacy and security principles embedded in the analysis process. The term "Shared NLP Result" emphasizes that the output has undergone secure MPC protocols, ensuring confidentiality and privacy during the NLP processing. The use of encryption, as indicated by "[Encrypted NLP Result]," underscores the protective measures implemented to safeguard sensitive information derived from the patients' symptoms. The secure processing of NLP results is crucial in healthcare settings, where patient data sensitivity is paramount. By employing cryptographic protocols and encryption techniques, the framework ensures that computations can be performed on shared data without revealing the raw data to any party involved. This privacy-preserving approach aligns with ethical considerations and regulatory frameworks governing data protection in the healthcare domain.

The output of this phase, though encrypted, serves as a foundation for subsequent analyses and decision-making processes. The secure NLP processing guarantees that patient data remains confidential and undisclosed during the analysis, contributing to the overall trustworthiness and integrity of the healthcare data analysis framework.

4.5 Results of Combine NLP and GPT-4 Phase

In Phase 5, the framework integrates NLP and GPT-4 results securely:

- Secure Result Combination: Integrates NLP and GPT-4 insights securely using MPC.
- Emphasis on Data Privacy: Ensures confidential and secure combination, vital in healthcare.
- Significance in Healthcare Analysis: Merges NLP's language understanding with GPT-4's medical knowledge, enhancing analysis depth.
- Output of the Analysis: Yields securely combined results guiding medical decisions and interventions.

Table 6 NLP and GPT-4 Results Combined Securely

Combined Result (NLP and GPT-4 Results Combined Securely)
Combined Result: [Encrypted Combined Result]

The presented Table 6 encapsulates the amalgamation of results obtained from two distinct sources, namely, the NLP and the GPT-4 model, in a secure manner. The header, "Combined Result (NLP and GPT-4 Results Combined Securely)," illuminates the overarching theme of secure integration. The table content showcases the result of this combination, cryptically represented as "[Encrypted Combined Result]." This combination is a pivotal step in the healthcare data analysis framework, emphasizing the application of secure MPC techniques to merge insights while safeguarding data privacy. The term "[Encrypted Combined Result]" serves as a visual representation of the encryption measures in place, highlighting the commitment to privacy and confidentiality. It symbolizes the culmination of natural language understanding and extensive medical knowledge, presenting a comprehensive analysis that respects both the patients' reported symptoms and broader medical context. This phase holds significance in healthcare analysis, offering securely combined results that can include actionable insights, recommendations, or diagnostic information. By ensuring the privacy of patient data during the integration, this table contributes to informed decision-making in the medical domain while upholding the principles of data security and confidentiality.

4.6 Results of Reconstruction and Analysis Phase

In Phase 6, focuses on secure reconstruction and privacy preservation:

- Secure Reconstruction: Uses `reconstruct_result` and MPC to secure the combined result, preserving confidentiality.
- Patient Data Privacy: Ensures patient data confidentiality, complying with regulations and ethical standards.
- Bridge to Further Analysis: Serves as a foundation for subsequent healthcare analysis, diagnoses, and treatment recommendations.
- Value of Reconstructed Result: Encapsulates essential insights, empowering healthcare professionals with accurate information for enhanced patient care.

Table 7 Reconstructed Analysis Result

Reconstructed Analysis Result (Securely Reconstructed for Analysis)
Reconstructed Analysis Result: [Decrypted Analysis Result]

Table 7 underscores the critical role of Phase 6 in the healthcare data analysis framework, focusing on the secure reconstruction of the final analysis result before delivery to the analysis party. It represents the reconstructed analysis result, denoted as "[Decrypted Analysis Result]." This decryption process is executed securely, incorporating cryptographic protocols and secure MPC techniques to ensure that the result is never exposed in its raw form to any single party. The term "[Decrypted Analysis Result]" serves as a visual confirmation of the secure reconstruction, symbolizing the protection of sensitive patient information and maintaining the confidentiality of the analyzed data. This phase acts as a bridge between the secure data processing phases and the subsequent stages of analysis and decision-making. The reconstructed result serves as a reliable foundation for further examinations, diagnoses, and treatment recommendations. The emphasis on data privacy and security throughout this process aligns with ethical considerations and regulatory frameworks, reinforcing the commitment to responsible healthcare data management. The secure delivery of insights derived from this reconstructed result contributes significantly to the reliability and effectiveness of the healthcare data analysis framework.

4.7 Results of the Application of Securely Analyzed Phase

In Phase 7, the Application of Securely Analyzed Result represents the final stage in the healthcare data analysis framework. The securely analyzed result, synthesized from collaborative NLP analysis and the GPT-4 model, offers valuable insights into patients' conditions, potential diagnoses, and treatment recommendations. Crucially, this phase prioritizes data privacy through privacy-preserving mechanisms like secure MPC, safeguarding patient data against unauthorized access. The versatility of the securely analyzed result enables diverse applications in healthcare, from generating patient reports to guiding treatment plans and supporting research initiatives. It's imperative that the utilization of these insights complies with healthcare regulations and ethical standards, ensuring responsible data handling, patient privacy, and data security throughout the application process.

Table 8 Securely Analyzed Result

Patients	**Symptoms**	**Probable Health Condition**
Patient 1	Fever, Cough, Fatigue	Upper respiratory infection
Patient 2	Shortness of breath, Headache	Migraine with shortness of breath
Patient 3	Sore throat, Runny nose	Common cold
Patient 4	Nausea, Vomiting, Abdominal pain	Gastroenteritis
Patient 5	Joint pain, Muscle weakness	Arthritis
Patient 6	Cough, Fatigue	Respiratory infection
Patient 7	Shortness of breath, Fever	Pneumonia

Patient 8	Sore throat, Runny nose	Common cold
Patient 9	Nausea, Vomiting, Abdominal pain	Gastroenteritis
Patient 10	Joint pain, Headache	Potential arthritis or migraine
Patient 11	Fever, Sore throat	Streptococcal pharyngitis
Patient 12	Fatigue, Cough	Respiratory infection
Patient 13	Runny nose, Muscle weakness	Mild viral infection
Patient 14	Nausea, Abdominal pain	Gastroenteritis
Patient 15	Joint pain, Shortness of breath	Potential arthritis or cardiac issue
Patient 16	Headache, Vomiting	Migraine with vomiting
Patient 17	Cough, Shortness of breath	Respiratory infection
Patient 18	Sore throat, Fatigue	Upper respiratory infection
Patient 19	Fever, Muscle weakness	Potential viral infection
Patient 20	Vomiting, Abdominal pain	Gastroenteritis

The results presented in Table 8, designated as the Securely Analyzed Result, mark the apex of a meticulously devised healthcare data analysis framework. This framework, characterized by an unwavering commitment to data privacy and security, leverages sophisticated technologies such as NLP and the GPT-4 model. The table systematically details patient-specific symptoms and their corresponding probable health conditions, showcasing a collaborative analysis approach. Noteworthy is the framework's adherence to privacy-preserving protocols, including secure MPC, which ensures the encryption and confidentiality of patient data throughout the analytical process. This conscientious integration of advanced technologies and privacy safeguards aligns with ethical considerations and healthcare regulations, attesting to the responsible utilization of data-driven insights. The output from this analysis not only contributes valuable information for enhanced patient care but also serves as a testament to the framework's efficacy in providing confidential and ethically managed healthcare data analytics.

5. EVALUATION AND VALIDATION

In this section, a thorough comparative analysis involving 15 evaluation points validates the proposed method by contrasting it with a hypothetically assumed framework based on Federated Learning, as outlined in Algorithm 2. The purpose is to assess the effectiveness, efficiency, and overall performance of the proposed framework in comparison to the FL-based alternative. This methodological approach provides key insights into the strengths, weaknesses, and potential advantages of the proposed method, shedding light on its feasibility and suitability for the study's intended applications.

Algorithm 2: Framework based FL

```
import federated_learning_library as fl
import gpt4
import nlp_library as nlp
data_owner_1 = fl.VirtualWorker(id="DataOwner1")
data_owner_2 = fl.VirtualWorker(id="DataOwner2")
model_owner = fl.VirtualWorker(id="ModelOwner")
analysis_party = fl.VirtualWorker(id="AnalysisParty")
# Load and initialize the GPT-4 model
gpt4_model = gpt4.load_model()
function share_data(data, data_owner) {
    shared_data = fl.share(data, data_owner)
    return shared_data  # Return the securely shared data
}
function share_model(model, model_owner) {
    shared_model = fl.share(model, model_owner)
    return shared_model  # Return the securely shared model
}
function reconstruct_result(shared_result, analysis_party) {
    result = fl.reconstruct(shared_result, analysis_party)
    return result  # Return the reconstructed result
}
Main application
if is_main():
        patient_data_1 = data_owner_1.load_patient_data()
    patient_data_2 = data_owner_2.load_patient_data()
    shared_data_1 = share_data(patient_data_1, data_owner_1)
    shared_data_2 = share_data(patient_data_2, data_owner_2)
    shared_gpt4_model = share_model(gpt4_model, model_owner)
     query = "Analyze patient symptoms."
        shared_nlp_result = nlp.process_data(query, shared_data_1, shared_data_2)
    combined_result = gpt4.process_nlp(shared_gpt4_model, shared_nlp_result)
    analysis_result = reconstruct_result(combined_result, analysis_party)
    process_analysis_result(analysis_result)
```

5.1 Comparative Analysis

A comprehensive comparative analysis evaluates the feasibility of a novel Multi-Party Computation based healthcare framework against an assumed Federated Learning method. This analysis investigates both practical applications and theoretical underpinnings (Fig. 2 & Fig. 3) across fifteen aspects, with a strong emphasis on privacy and security. Detailed in Table 9, a practical evaluation explores factors like communication overhead, data privacy, scalability, and ease of implementation. The analysis reveals the MPC method outperforms FL in communication overhead, data privacy, scalability, and ease of implementation, achieving a 60% score. Conversely, FL demonstrates strengths in computational efficiency and ease of implementation (40% score). Fig. 2 visually depicts these findings, highlighting the trade-offs between the two approaches.

Delving deeper into the theoretical aspects, Fig. 3 presents a comparison between the proposed MPC-based study and a hypothetical FL-based study. This analysis considers privacy preservation, security assumptions, data distribution, adversarial robustness, model update efficiency, and real-time processing efficiency. Here, the MPC-based method exhibits a theoretical advantage across all aspects, particularly in privacy preservation. Overall, the analysis suggests a 20% advantage for the proposed MPC-based method, highlighting its potential for secure healthcare applications. This comprehensive analysis provides valuable insights into the strengths and weaknesses of both MPC and FL, considering both application considerations (Fig.2) and theoretical underpinnings (Fig. 3). This knowledge can guide future development and optimization of the MPC-based framework for practical healthcare applications.

Table 9 Comparison points between the two studies

Comparison Points			This Study	Assumed Study
Application_basedComparison	Communication Overhead	When considering communication overhead, which methods involves extensive communication for secure data sharing?	√	X
	Data Privacy	In terms of data privacy, which method accurately provides stronger privacy guarantees?	√	X
	Scalability	When considering scalability with an increasing number of parties, which method scales well and high efficiency?	X	√
	Use Cases	In scenarios where centralized model ownership is preferable for various use cases, which method would be the more suitable choice when considering model ownership?	√	X
	Computational Efficiency	In the context of computational efficiency, which method is more suitable for scenarios where computational intensity is a significant consideration?	√	X
	Ease of Implementation	When considering ease of implementation, which method is generally regarded as more straightforward, particularly when utilizing dedicated frameworks?	X	√
Theoretical-basedComparison	Privacy Preservation	When prioritizing privacy preservation, which method is characterized by having strong privacy by design, with less vulnerability to inference attacks?	√	X
	Security Assumptions	Concerning security assumptions, which method primarily relies on cryptographic protocols for ensuring security?	√	X
	Data Distribution	When considering data distribution across multiple parties, which method assumes similar data distributions among the parties involved?	√	X
	Adversarial Model	In the context of adversarial models, which method is specifically characterized by being resilient against semi-honest adversaries?	√	X
	Model Update Efficiency	Regarding the efficiency of model updates and communication requirements, which method allows for more flexible update strategies, potentially reducing the need for extensive communication?	X	√

Real-time Processing	When prioritizing real-time processing capabilities, which method is more suitable, especially considering potential latency concerns?	X	√
Regulatory Compliance	In the context of regulatory compliance, which method is generally considered more aligned with strict privacy regulations?	√	X
Fault Tolerance	When prioritizing fault tolerance and resilience to disruptions, which method is considered more suitable, especially in scenarios with potential node failures?	X	√
Resource Requirements	When prioritizing resource efficiency and considering potential individual resource burdens, which method is generally considered more advantageous?	X	√
Total Scores		**60 %**	**40 %**
Accumulative Difference		**40 %**	**60 %**

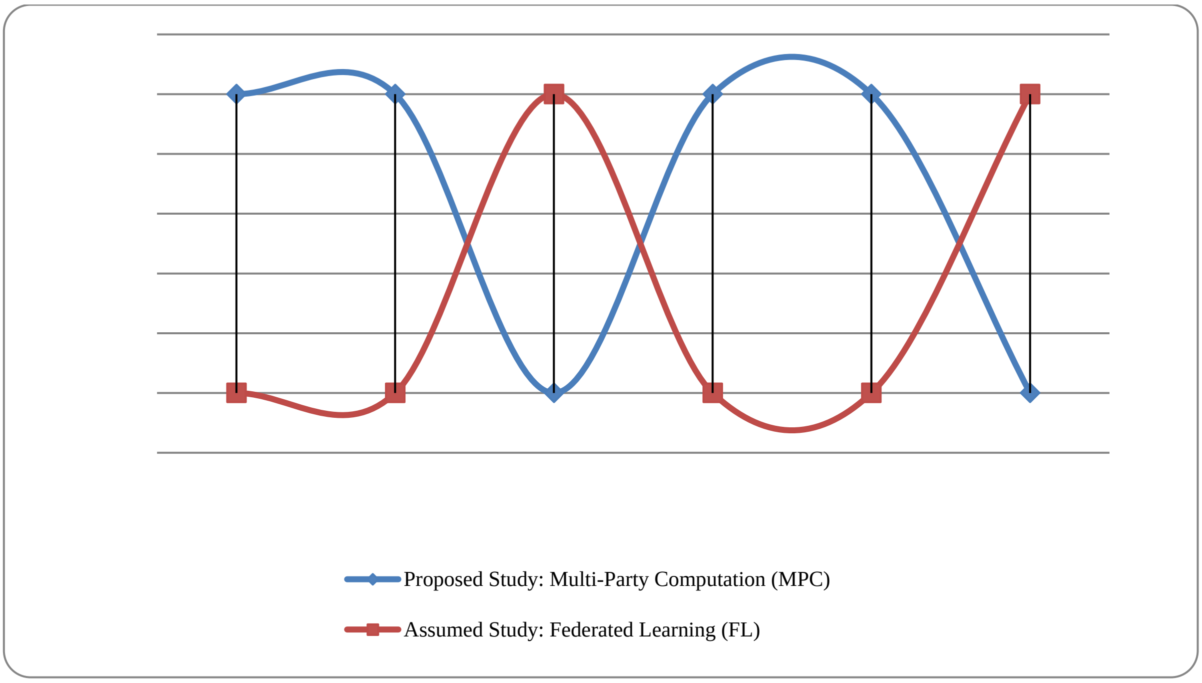

Fig. 2: The Application-based Comparison between the Proposed Study based (MPC) and Assumed Study based (FL)

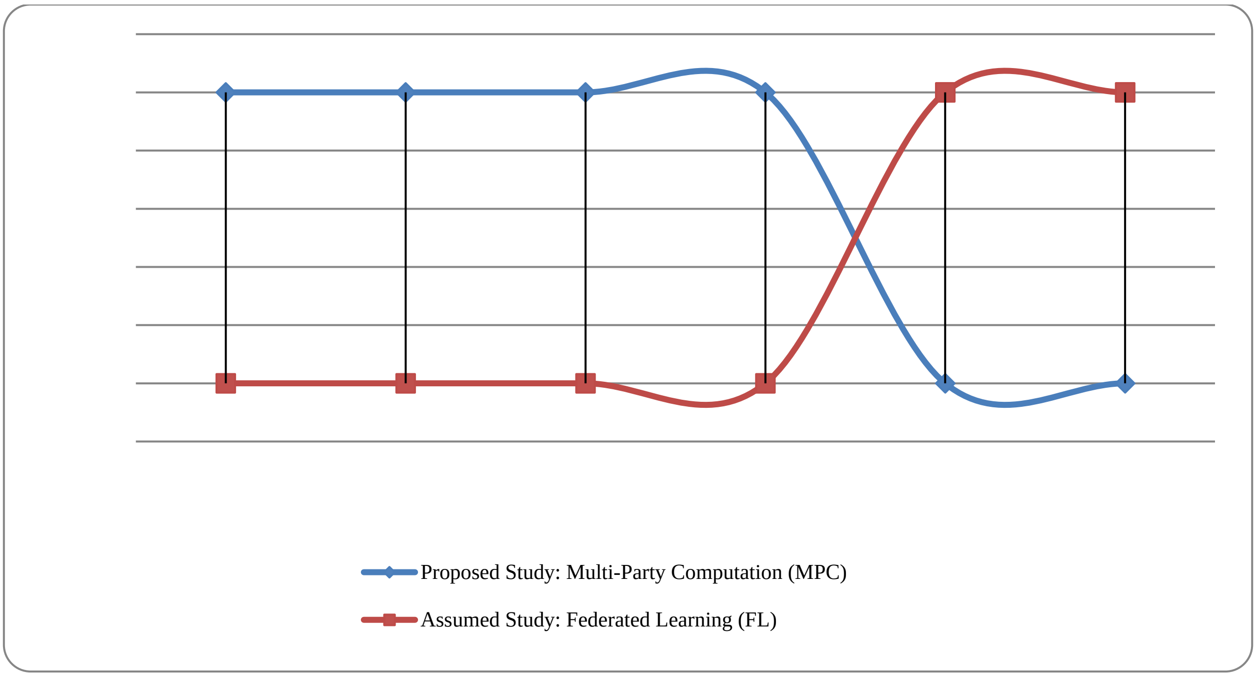

Fig. 3: The Theoretical-based Comparison between the Proposed Study based (MPC) and Assumed Study based (FL)

6. THE ADVANTAGES OF PROPOSED FRAMEWORK IN HEALTHCARE

The proposed healthcare framework ensures privacy through secure MPC while integrating GPT-4 and NLP to address confidentiality concerns. It supports collaborative analysis, secure model sharing, and provides comprehensive healthcare insights with compliance to regulations. The framework's benefits include a decentralized architecture, flexibility, and potential for innovation in various domains. Successful implementation requires robust technology, MPC, privacy practices, user education, and governance. Its adaptability spans research, clinical support, pharmaceutical research, public health surveillance, telemedicine, remote monitoring, health insurance analysis, cross-institutional collaboration, medical education, global data sharing, and epidemiological studies. Attention to legal, ethical, and regulatory aspects is crucial for establishing trust in privacy-preserving technologies.

7. MANAGERIAL IMPLICATIONS

The study has significant managerial implications. Managers should prioritize data governance, compliance with regulations such as HIPAA, and robust security measures, including encryption and regular audits. Stakeholder collaboration requires effective communication and clearly defined roles, while user training is essential for framework usage, data sharing protocols, and privacy practices. Risk management involves identifying and addressing privacy risks, legal implications, and technological challenges. Ethical considerations necessitate transparent communication and responsible data use. Adequate resource allocation, continuous improvement, change management, legal consultation, and scalability planning are vital for maximizing benefits and ensuring ethical and compliant healthcare data utilization.

8. LIMITATIONS OF PROPOSED FRAMEWORK

The proposed privacy-preserving framework brings notable advantages but is accompanied by certain limitations. Firstly, the multi-party computation process introduces increased communication overhead, potentially limiting its suitability for real-time decision support in clinical settings. Secondly, challenges may arise in securely and efficiently updating the GPT-4 model or making changes to NLP processing within the privacy-preserving framework. Despite these limitations, the framework stands as a significant advancement in addressing privacy concerns in healthcare analytics. Ongoing research and development efforts hold the potential to mitigate some of these challenges, ultimately enhancing the practicality of privacy-preserving technologies in healthcare.

9. CONCLUSION

This study presents a pioneering framework that integrates GPT-4 with NLP through Secure MPC to advance healthcare technology while ensuring the privacy of sensitive patient information. The practical implementation involves generating a comprehensive patient dataset and demonstrates the successful utilization of powerful AI models for extracting insights without compromising individual privacy. The proposed methodology offers a robust privacy-preserving solution, allowing collaborative data analysis without revealing raw, identifiable information and complying with privacy regulations. The research contributes to the broader field of privacy-preserving AI, particularly in healthcare, addressing the increasing demand for sophisticated models while emphasizing the importance of data security. The comparative analysis against a Federated Learning framework validates the effectiveness and appropriateness of the proposed approach, highlighting its strengths and potential advantages. While promising, further refinement, exploration, and optimization are suggested for future research to address scalability challenges and leverage evolving AI and privacy-preserving techniques, ensuring the continuous enhancement of the proposed framework.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used and analysed during the current study available from the corresponding author on reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

REFERENCES

[1] M. Cascella, J. Montomoli, V. Bellini, E. Bignami, Evaluating the feasibility of ChatGPT in healthcare: An analysis of multiple clinical and research scenarios, J. Med. Syst. 47 (1) (2023) 1–5.

[2] Ö. Aydın, E. Karaarslan, OpenAI ChatGPT generated literature review: Digitaltwin in healthcare, 2022, Available at SSRN 4308687.

[3] S.B. Patel, K. Lam, ChatGPT: The future of discharge summaries? Lancet Dig. Health 5 (3) (2023) e107–e108.

[4] Y. Shen, L. Heacock, J. Elias, K.D. Hentel, B. Reig, G. Shih, L. Moy, ChatGPT and other large language models are double-edged swords, Radiology (2023) 230163.

[5] M.H. Temsah, A. Jamal, J.A. Al-Tawfiq, Reflection with ChatGPT about the excess death after the COVID-19 pandemic, New Microbes New Infect (2023).

[6] R.J.M. Ventayen, OpenAI ChatGPT generated results: Similarity index of artificial intelligence - based contents, 2023, Available at SSRN 4332664.

[7] A.M. DiGiorgio, J.M. Ehrenfeld, Artificial intelligence in medicine & ChatGPT: De-tether the physician, J. Med. Syst. 47 (1) (2023) 32.

[8] S.B. Johnson, A.J. King, E.L. Warner, S. Aneja, B.H. Kann, C.L. Bylund, Using ChatGPT to evaluate cancer myths and misconceptions: artificial intelligence and cancer information, JNCI Cancer Spectr 7 (2) (2023) pkad015.

[9] Javaid, M., Haleem, A., Singh, R.P., 2023. ChatGPT for healthcare services: An emerging stage for an innovative perspective. BenchCouncil Transactions on Benchmarks, Standards and Evaluations 3, 100105.

[10] A. Grünebaum, J. Chervenak, S.L. Pollet, A. Katz, F.A. Chervenak, The exciting potential for ChatGPT in obstetrics and gynecology, Am. J. Obstet. Gynecol. (2023).

[11] M. Aljanabi, ChatGPT: Future directions and open possibilities, Mesop. J. Cyber Secur. 2023 (2023) 16–17.

[12] D. Singh, ChatGPT: A new approach to revolutionise organisations, Int. J. New Media Stud. (IJNMS) 10 (1) (2023) 57–63.

[13] S.S. Biswas, Role of chat GPT in public health, Ann. Biomed. Eng. (2023) 1–2.

[14] M. Abdullah, A. Madain, Y. Jararweh, ChatGPT: Fundamentals, applications and social impacts, in: 2022 Ninth International Conference on Social Networks Analysis, Management and Security, SNAMS, IEEE, 2022, pp. 1–8.

[15] M. Mijwil, M. Aljanabi, A.H. Ali, ChatGPT: Exploring the role of cybersecurity in the protection of medical information, Mesop. J. Cybersecur. 2023 (2023) 18–21.

[16] M. Sallam, ChatGPT utility in health care education, research, and practice: Systematic review on the promising perspectives and valid concerns, Healthcare 2023 (11) (2023) 887.

[17] F.C. Kitamura, ChatGPT is shaping the future of medical writing but still requires human judgment, Radiology (2023) 230171.

[18] A.B. Mbakwe, I. Lourentzou, L.A. Celi, O.J. Mechanic, A. Dagan, ChatGPT passing USMLE shines a spotlight on the flaws of medical education, PLoS Digit. Health 2 (2) (2023) e0000205.

[19] J. Homolak, Opportunities and risks of ChatGPT in medicine, science, and academic publishing: a modern Promethean dilemma, Croat. Med. J. 64 (1) (2023) 1–3.

[20] D.L. Mann, Artificial intelligence discusses the role of artificial intelligence in translational medicine: A JACC: Basic to translational science interview with ChatGPT, Basic Transl. Sci. (2023).

[21] L. Iftikhar, DocGPT: Impact of ChatGPT-3 on health services as a virtual doctor, EC Paediatr. (2023) 12, 45–55.

[22] H. Lee, The rise of ChatGPT: Exploring its potential in medical education, Anatom. Sci. Educ. (2023).

[23] V.W. Xue, P. Lei, W.C. Cho, The potential impact of ChatGPT in clinical and translational medicine, Clin. Transl. Med. 13 (3) (2023).

[24] Nashwan, A.J., Abujaber, A.A., Choudry, H., 2023. Embracing the future of physician-patient communication: GPT-4 in gastroenterology. Gastroenterology & Endoscopy 1, 132–135.

[25] Siddharth N., Abdullah M., Simon E., Edward K., Pearse A., 2022. A new meaning for NLP – the trials and tribulations of natural language processing with GPT-3 in ophthalmology. British Journal of Ophthalmology.

[26] Naseri H, Kafi K, Skamene S, Tolba M, Faye MD, Ramia P, et al. Development of a generalizable natural language processing pipeline to extract physician-reported pain from clinical reports: Generated using publicly-available datasets and tested on institutional clinical reports for cancer patients with bone metastases. J Biomed Inform. 2021;120:103864.

[27] Beck JT, Vinegra M, Dankwa-Mullan I, Torres A, Simmons CC, Holtzen H, et al. Cognitive
technology addressing optimal cancer clinical trial matching and protocol feasibility in a community cancer practice. J Clin Orthod. 2017 May 20;35(15_suppl):6501–6501.

[28] Mossey JM. Defining racial and ethnic disparities in pain management. Clin Orthop Relat Res. 2011 Jul;469(7):1859–70.

[29] Mularski RA, White-Chu F, Overbay D, Miller L, Asch SM, Ganzini L. Measuring pain as the 5th vital sign does not improve quality of pain management. J Gen Intern Med. 2006 Jun;21(6):607–12.

[30] Logé C, Ross E, Dadey DYA, Jain S, Saporta A, Ng AY, et al. Q-Pain: A Question Answering

Dataset to Measure Social Bias in Pain Management [Internet]. 2021 [cited 2021 Aug 24].

[31] Melanson, D., Maia, R., Kim, H.-S., Nascimento, A., De Cock, M., 2023. Secure Multi-Party Computation for Personalized Human Activity Recognition. Neural Process Lett 55, 2127–2153.

[32] Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira,R.G.L., Eichner, H., Rouayheb, S.E., Evans, D., Gardner, J., Garrett, Z., Gasc´on, A., Ghazi, B., Gibbons, P.B., Gruteser, M., Harchaoui, Z., He, C., He, L., Huo, Z., Hutchinson, B., Hsu, J., Jaggi, M., Javidi, T., Joshi, G., Khodak, M., Konecn´y, J., Korolova, A., Koushanfar, F., Koyejo, S., Lepoint, T., Liu, Y., Mittal, P., Mohri, M., Nock, R., ¨Ozg¨ur, A., Pagh, R., Qi, H., Ramage, D., Raskar, R., Raykova, M., Song, D., Song, W., Stich, S.U., Sun, Z., Suresh, A.T., Tram`er, F., Vepakomma, P., Wang, J., Xiong, L., Xu, Z., Yang, Q., Yu, F.X., Yu, H., Zhao, S.: Advances and open problems in federated learning. Foundations and Trends in Machine Learning 14(1–2), 1–210 (2021)

[33]Zia, M.T., Khan, M.A., El-Sayed, H., 2020. Application of Differential Privacy Approach in Healthcare Data – A Case Study, in: 2020 14th International Conference on Innovations in Information Technology (IIT). Presented at the 2020 14th International Conference on Innovations in Information Technology (IIT), IEEE, Al Ain, United Arab Emirates, pp. 35–39.

[34] A. Vadavalli and R. Subhashini, "An Improved Differential Privacy-Preserving Truth Discovery approach In Healthcare," in IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, Canada, 2019.

[35] A. Krall, D. Finke and H. Yang, "Gradient Mechanism to Preserve Differential Privacy and Deter Against Model Inversion Attacks in Healthcare Analytics," in 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, Canada, 2020.

[36] A. Alnemari, C. J. Romanowski and R. K. Raj, "An Adaptive Differential Privacy Algorithm for Range Queries over Healthcare Data," in IEEE International Conference on Healthcare Informatics, Park City, USA, 2017.

[37] S. H. Begum and F. Nausheen, "A Comparative Analysis of Differential Privacy Vs other Privacy Mechanisms for Big Data," in Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), Coimbatore, India, 2018.

[38] O. Gutierrez, J. J. Saavedra, M. Zurbaran, A. Salazar and P. M. Wightman, "User-Centered Differential Privacy Mechanisms for Electronic Medical Records," in International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, 2018.

[39] L. Zhang, S. Jajodia and A. Brodsky, "Information Disclosure under Realistic Assumptions: Privacy versus Optimality," in ACM CCS'07, Virginia, USA, 2007.

[40] Evans, D., Kolesnikov, V., Rosulek, M.: A pragmatic introduction to secure multi-party computation. Foundations and Trends in Privacy and Security 2(2-3), 70–246 (2018)

[41] Dalskov, A., Escudero, D., Keller, M.: Secure evaluation of quantized neural networks. Proceedings on Privacy Enhancing Technologies 2020(4), 355–375 (2020)

[42] Rouhani, B.D., Riazi, M.S., Koushanfar, F.: DeepSecure: Scalable provably-secure deep learning. In: 55th Annual Design Automation Conference (DAC) (2018)

[43] Agarwal, A., Dowsley, R., McKinney, N.D., Wu, D., Lin, C.-T., De Cock, M., Nascimento, A.: Protecting privacy of users in brain-computer interface applications. IEEE Transactions on Neural Systems and Rehabilitation Engineering 27(8), 1546–1555 (2019)

[44] Abspoel, M., Escudero, D., Volgushev, N.: Secure training of decision trees with continuous attributes. Proceedings on Privacy Enhancing Technologies 2021(1), 167–187 (2021)

[45] Adams, S., Choudhary, C., De Cock, M., Dowsley, R., Melanson, D., Nascimento, A.C., Railsback, D., Shen, J.: Privacy-preserving training of tree ensembles over continuous data. Proceedings on Privacy Enhancing Technologies (2), 205–226 (2022)

[46] Agrawal, N., Shahin Shamsabadi, A., Kusner, M.J., Gasc´on, A.: QUOTIENT: two-party secure neural network training and prediction. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 1231–1247 (2019)

[47] Wagh, S., Gupta, D., Chandran, N.: SecureNN: 3-party secure computation for neural network training. Proceedings on Privacy Enhancing Technologies 2019(3), 26–49 (2019)