Homomorphic Encryption-Based Testing for Secure Mobile Healthcare Data Processing in 5G-Enabled Systems

Basava Ramanjaneyulu Gudivaka

Raas Infotek, Newark Delaware, USA

basava.gudivaka537@gmail.com

Rajya Lakshmi Gudivaka

Wipro, Hyderabad, Telangana, India

rlakshmigudivaka@gmail.com

Raj Kumar Gudivaka

Birla soft Limited, Hyderabad, Telangana, India

rajkumargudivaka35@gmail.com

Dinesh Kumar Reddy Basani

CGI, British Columbia, Canada

dinesh.basani06@gmail.com

Sri Harsha Grandhi

Intel Corporation, Folsom, California, USA

grandhi.sriharsha9@gmail.com

Sundarapandian Murugesan

Intel Corporation, Folsom, CA, USA

tmsundaroff@gmail.com

M M Kamruzzaman
Department of Computer Science,
College of Computer and Information Sciences, Jouf University, Sakakah, Saudi Arabia

mmkamruzzaman@ju.edu.sa

ABSTRACT

The advancement of 5G-enabled mobile healthcare systems has improved real-time patient monitoring, diagnostics, and data security. However, ensuring privacy-preserving data processing remains a challenge. This study proposes a Homomorphic Encryption-Based Testing framework integrating Fully Homomorphic Encryption (FHE), Secure Multiparty Computation (MPC), and AI-driven analytics for secure mobile healthcare data processing. The proposed method incurs encryption (2.1 ms), decryption (2.6 ms), processing latency (4.7 ms), computational overhead (15.7%), and the data transmission efficiency is 48.3 Mbps, which considerably surpasses the traditional encryption methods. The framework supports privacy-preserving AI-driven diagnostics in real time over 5G networks encrypted data, therefore HIPAA and GDPR-compliant. Future work includes (1) optimizing computation efficiency, (2) exploring expanded federated learning securely, and (3) enhancing real-time encrypted AI-driven healthcare analytics.

Keywords: Homomorphic Encryption, Secure Multiparty Computation, 5G Cloud Computing, Privacy-Preserving Healthcare, AI-driven Analytics, Federated Learning, Real-Time Diagnostics.

1. INTRODUCTION

With the widespread development of 5G-enabled mobile healthcare systems **Qureshi et al. (2020),** real-time patient monitoring, diagnostics, and treatment have improved efficiency and are more accessible. The Internet of Medical Things has greatly contributed to seamless data transfer between wearable devices, medical sensors, and cloud-based **Thamilarasu et al. (2020)** healthcare platforms. These technologies allow healthcare providers to access data in real time, improve care for patients, and implement predictive analytics for the early detection of diseases. The mobile healthcare interconnecting ecosystem poses very critical issues on security and privacy. It deals with a high level of patient data that has to be strictly protected from any unauthorized access, cyberattack, or even breach.

The mobile healthcare platform has security vulnerability issues due to the high amounts of data transferring between IoMT devices and the cloud storage **Yang et al. (2020)** facilities, making their records vulnerable to hacking and other forms of unauthorized access. The symmetrical and asymmetric encryption techniques represent traditional encryption algorithms that offer data security resting and in transmission but fail in computing data integrity, which subjects the healthcare information to possible compromises when accessed online for remote diagnostic procedures, artificial intelligence-based analytical processing, or even cloud computation. Ensuring data privacy and integrity during computational operations is a significant challenge that must be addressed for the successful deployment of secure mobile healthcare systems. Homomorphic encryption (HE) is a new cryptographic approach to overcome these security challenges. HE enables mathematical operations on encrypted data without decryption, thus providing privacy-preserving computations. This property allows secure data analysis, AI model training, and diagnostic decision-making without violating data confidentiality. Testing using homomorphic encryption-based testing is specifically useful for privacy-preserving machine learning, in which AI models can be trained and tested on encrypted healthcare datasets without exposing raw patient information.

Integration of HE and 5G-enabled mobile healthcare systems might significantly improve security. With connectivity at the levels of 5G networks having low latency for real-time access to encrypted diagnoses, AI analysis, and peer-to-peer interfaces between health caregivers and patients in real-time data exchange, its homomorphic encrypting property maintains the privacy-preserved AI training environment. From data collection via IoMT devices to cloud processing and transmission through 5G networks, HE provides end-to-end security in order not to compromise data breaches, unauthorized access, and cyber threats. Homomorphic encryption-based testing **Paul et al. (2021)** in mobile healthcare is scalable, secure, and efficient. HE lays a foundation for trusted healthcare services, regulatory compliance, and improved patient data protection by addressing the security and privacy concerns of traditional encryption techniques. The growing demand for AI-driven diagnostics, remote monitoring, and telemedicine calls for HE-based security solutions to strengthen data privacy and trust in next-generation mobile healthcare ecosystems. Homomorphic encryption-based testing is the secure approach for data processing. It facilitates the computation directly on encrypted patient data without decrypting it. Hence, healthcare analysis in real-time, AI-driven diagnostics, and privacy-preserving machine learning become possible. Contrary to conventional encryption, HE enables health systems to securely process sensitive data without exposing it to unauthorized parties. It trains AI models on analytics **Nasr et al. (2021)** while still keeping the data of patients private, thus surmounting a major concern limiting the adoption of AI in health care. Its applications are vast in remote patient monitoring, disease prediction, and clinical decision support, ensuring the data is encrypted from collection to cloud analytics and across 5G networks. Maintaining end-to-end encryption, HE minimizes the risks of cyberattacks, unauthorized access, and data breaches. It also provides HIPAA, GDPR, and global healthcare compliance, thus ensuring a scalable and secure solution to protect patient records while enabling efficient mobile healthcare data processing.

Objectives:

- Enhance data privacy and security through the implementation of homomorphic encryption and end-to-end encryption in mobile healthcare systems.
- Enable privacy-preserving computation in AI-driven diagnostics, real-time analytics, and decision-making healthcare applications.
- Optimize computational efficiency in 5G-enabled healthcare systems by reducing processing overhead and improving scalability for real-time applications.
- Ensure adherence to healthcare regulations such as HIPAA and GDPR while maintaining data integrity to prevent unauthorized alterations.
- Evaluate the performance of homomorphic encryption-based testing by assessing computational efficiency, security, and accuracy in comparison to traditional encryption methods.

Kumar et al. (2020) suggested a Secure Multiparty Computation (MPC) enabled e-healthcare system integrated with Homomorphic Encryption (HE) for privacy-preserving data sharing and secure remote diagnostics. Though their approach has tackled the data confidentiality and security issue, still considerable gaps remain in scalability, computational efficiency, and real-time processing for large-scale healthcare systems. The present models lack optimized encryption techniques that would handle high-volume medical data processing without any latency issues. Integration of AI-driven diagnostics with encrypted computations for real-time predictive healthcare analytics is limited. The proposed framework does not explore secure interoperability across various institutions to enable efficient patient record sharing. Future research work should accordingly address these limitations of providing lightweight encryption, AI-driven diagnostics, and cross-institutional secure data exchange for robust privacy-preserving e-healthcare systems.

Sinha et al. (2020) further identify privacy threats in public health surveillance systems wherein storing and sharing personal medical information becomes a cause of significant vulnerability. Traditional forms of encryption mandate decryption before a computation can take place, leading to increased risk in sensitive health data. These issues prevent appropriate contact tracing as well as response time to critical public health problems that were exemplified during the COVID-19 pandemic. The proposed Fully Homomorphic Encryption privacy-preserving mechanism would ensure calculations on the ciphertext without decrypting the same and would not achieve such capability in the present state of public health systems, a strong, scalable, and computational FHE model is in utmost need to safeguard healthcare data from the various entities.

2. LITERATURE SURVEY

Khan et al. (2020) proposed a secure authentication and encryption framework for IoT-based medical sensor data, integrating SHA-512 for integrity and improved ECC (IECC) for enhanced security. Their framework compared with RSA and ECC had lower computational costs and faster encryption/decryption times, ensuring efficient and secure patient data transmission in mobile healthcare.

Visconti et al. (2021) discussed FPGA-based solutions for high-throughput data processing and encryption in 5G networks, where applications are based on C-RAN accelerators, NFV-based network slicing, cognitive radio, and MIMO characterization. They implemented AES-128 encryption on the Xilinx Zynq Ultrascale+ MPSoC ZCU102 FPGA, which achieves high efficiency and optimized hardware utilization compared to the existing solutions.

Surendar (2020) presented a real-time big data analytics framework that integrated AI techniques for optimizing healthcare data streams. The study focused on improving data processing efficiency, predictive analytics, and decision-making in healthcare environments. The proposed model showed better accuracy, scalability, and real-time insights for the effective management of data for patient care and clinical diagnostics.

Hewa et al. (2020) suggested a secure telehealth system incorporating MEC and blockchain with 5G and IoT for the real-time data privacy, integrity, and authenticity. They adopted ECQV certificates and offloading storage to scale the solution and implemented a blockchain-based incentive mechanism for the data sharing process. They also tested the solution using Hyperledger Fabric and simulation of medical sensor using Raspberry Pi.

Mohanarangan et al. (2020) elaborated on enhanced security controls of cloud computing, focusing on enhancing data privacy and access control besides countering threats from cybercrimes. It was suggested in the study to have advanced mechanisms of encryption techniques and multi-level security frameworks protecting patient information under cloud-based health care systems, thus ensuring effective integrity and reliability of data toward security breaches along with compliance by health care norms.

Kumar et al. (2021) proposed a security and privacy-aware Artificial Intrusion Detection System using Federated Machine Learning for Beyond 5G edge networks. They incorporated Paillier

Homomorphic Encryption and differential privacy for enhanced data security. An Artificial Immune Intrusion Detection System was designed to classify anomalies, ensuring secure data transmission. Experimental results demonstrated its superior performance over existing edge security models.

Panga (2021) utilized techniques of machine learning and deep learning to focus on the determination of fraudulent healthcare claims, including billing anomalies and suspicious transactions. The proposal is to propose AI-driven models for enhancing accuracy in fraud detection while minimizing false positives and responsibly informing healthcare financial decisions to improve efficiency in the prevention of fraud and financial security.

Wang et al. (2021) suggested a deep learning-based data privacy protection model for AIoT systems, utilizing homomorphic encryption and secure MPC. Their technique provides encrypted processing of data in a way that no user could gain access to model parameters; meanwhile, data remains private. The experimental analysis indicated high accuracy for classification tasks and is hence considered a promising solution for safe AI-driven IoT applications.

Sitaraman (2021) studied AI-driven healthcare systems in advanced data analytics and mobile computing, focusing on real-time monitoring of patients, predictive diagnostics, and decision support. The key findings of this study were: AI optimizes healthcare workflows that are efficient and scalable, facilitating data-driven decisions and thus achieving better patient care and operational efficacy.

Rahman et al. (2021) proposed a secure, private, and explainable IoHT framework for sustainable health monitoring in smart cities. Their model incorporates private blockchain for secure model aggregation, and federated learning for encrypted data sharing, and explains the ability for social acceptance. The approach ensures data privacy, security, and trustworthiness while allowing scalable and sustainable IoHT-enabled healthcare applications.

Suraci et al. (2021) proposed a secure and lightweight 6G eHealth system that integrates Multi-Access Edge Computing (MEC) and Device-to-Device (D2D) communication for low-latency and high-reliability healthcare services. Their architecture enhances secure data management for IoMT devices, ensuring efficient telemonitoring. Preliminary evaluations demonstrated improved security and reduced latency, making it a promising solution for future eHealth systems.

Xu et al. (2020) designed a blockchain-enabled accountability mechanism for preventing information leakage in vertical industry services within 5G networks. Their scheme combines homomorphic encryption for secure watermarking and removes the reliance on Trusted Third Parties (TTP). The system allows secure and fair content sharing while efficient tracking of unauthorized data leaks improves security in mobile telemedicine and content-sharing services.

Feng et al. (2021) proposed blockchain-empowered decentralized horizontal federated learning with 5G-enabled UAVs to mitigate potential privacy risks and centralization vulnerability, as well as communication hurdles. Their architecture utilizes multi-signature smart contracts for cross domain authentication and the decentralized aggregation of models, reducing the dependency of a central server. Experimental findings show high efficiency in authentication processes and robust accuracy in models achieved for secure, scalable federated learning in networks of UAVs.

Xue et al. (2021) proposed a privacy-preserving and resource-efficient edge-computing-enabled clinical decision system using Federated Reinforcement Learning. Their framework integrates Mobile-Edge Computing and Software-Defined Networking, thereby optimizing the computation and storage across edge nodes. A fully decentralized federated framework, enhanced with double deep Q-networks (DDQN) enhances the clinical decision-making efficacy, while homomorphic encryption provides privacy protection of electronic medical records during training.

Singh and Chatterjee (2021) proposed a smart healthcare system called edge computing to improve data security and privacy with real-time response. Their architecture consists of an additional layer of edge computing for reducing latency and privacy preserving data through secure processing using Privacy-Preserving Searchable Encryption (PPSE). Finally, an access control mechanism prevents illegal access thereby providing better security and efficiency compared to cloud-based models of healthcare.

Rahman et al. (2020) proposed a secure and provenance-enhanced IoHT framework where blockchain-managed federated learning and differential privacy for data security and authentication are integrated. Their approach uses smart contracts for trust management, model distribution, and edge authentication. The framework supports full encryption of datasets and model training, thereby ensuring privacy-preserving decentralized IoHT-based health management while also being successfully validated for their clinical trial application.

Lin et al. (2020) presented a privacy-enhanced data fusion strategy for IoMT-based applications in COVID-19, focusing on secure processing of data and maintaining user privacy. Their framework combines sensitive task classification, assessment of task completion, incentive-based contracts, and homomorphic encryption to improve the reliability of data and participation. The simulation results show high accuracy in task performance and improved protection of privacy, thus making it a robust solution for IoMT-based applications for COVID-19.

El Azzaoui et al. (2020) proposed Block5GIntell, a blockchain-integrated AI framework for secure and intelligent 5G networks. Their approach enhances data analytics, security, and resource management by leveraging blockchain's decentralized nature. The framework improves AI-based network operations, addressing security challenges and efficiency concerns. A case study demonstrated energy savings at the RAN level, highlighting blockchain's role in optimizing AI-driven 5G environments.

Zheng et al. (2021) introduced a federated learning-based communication model for IoMT in MEC, addressing the high latency and communication overload issues. They also created a gradient reduction algorithm to minimize the cost of the iterations. The proposed algorithm maintains accuracy while reducing the updates. Experimental validation was carried out using linear and logistic regressions, which provided a significant reduction in communication costs compared to typical federated learning models.

Sitaraman (2020) explores the optimization of healthcare data streams using real-time big data analytics and artificial intelligence (AI) techniques. It discusses methods for efficiently processing large-scale healthcare data, enabling better decision-making, improved patient care, and the optimization of healthcare delivery systems.

Vasamsetty and Kaur (2021) that proposes a cloud computing-based framework using Particle Swarm Optimization with Time-Varying Acceleration Coefficients (PSO-TVAC) to optimize healthcare data analysis. This modification is considered to be an optimizer in the area of medical data processing that would help to build better-quality decisions for effective usage of resources in a health system.

Yalla (2021) discusses a cloud-based attribute-based encryption (ABE) approach for securing financial data. The paper explores the integration of ABE with big data technologies to enhance data confidentiality, access control, and security in financial systems, ensuring secure storage, processing, and retrieval of sensitive financial information.

Poovendran (2020) explores the implementation of the AES (Advanced Encryption Standard) encryption algorithm to enhance data security in cloud computing. The paper discusses the effectiveness of AES in safeguarding sensitive data during storage and transmission, emphasizing its robustness in protecting against cyber threats and ensuring confidentiality in cloud environments.

Narla et al. (2021) explore enhancing predictive healthcare modeling using advanced machine learning algorithms—Histogram-Based Gradient Boosting, MARS, and SoftMax Regression—in a cloud computing environment. The study demonstrates significant improvements in prediction accuracy, precision, and recall, offering an optimized solution for healthcare decision-making and outcomes.

Valivarthi, et al. (2021) propose an integrated BBO-FLC and ABC-ANFIS system for healthcare predictions, leveraging cloud computing and AI techniques. The model combines IoT-enabled sensors, fuzzy logic, and optimization algorithms to enhance disease prediction accuracy and real-time monitoring. It achieved 96% accuracy, with improved scalability and efficiency.

Natarajan (2018) proposes a hybrid model combining Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) to optimize Recurrent and Radial Basis Function Networks (RBFN) for healthcare disease detection. The model enhances accuracy and reduces processing time, offering a robust solution for real-time disease diagnosis, especially for chronic conditions.

Budda (2021) has proposed an overarching framework that consolidates Artificial Intelligence, Big Data Mining, and IoT to advance healthcare performance. The strategy emphasizes predictive analytics enhancement, patient care, resource allocation, and sustainability. It presents a revolutionary solution for real-time data processing, customized care, and effective delivery of healthcare.

Samudrala (2020) introduces an AI-based anomaly detection system for protecting healthcare data exchanges on multi-cloud environments. The system applies machine learning and cryptographic methods to identify anomalies in real-time, maintaining data integrity, privacy, and adherence to healthcare standards such as HIPAA. It has high detection rates and low false positives.

Sitaraman (2021) brings in Crow Search Optimization (CSO) to improve AI-based disease diagnosis in intelligent healthcare systems. CSO optimizes deep learning models, such as CNNs and LSTMs, with the advantage of increasing accuracy, precision, and recall. It surpasses conventional methods like GA and PSO and can be used as a dynamic tool for personalized and effective healthcare.

Panga (2021) investigates the use of machine learning and deep learning algorithms for detecting financial fraud in healthcare. The research indicates that Decision Tree Classifier, among other models, was able to achieve 99.9% accuracy in detecting fraudulent activities, which was more effective than using CNNs and RNNs, thus enhancing the integrity and financial security of healthcare systems.

Thirusubramanian (2021) proposes a machine learning-based AI methodology for financial fraud detection in IoT systems. The article underscores the efficacy of AI algorithms in monitoring financial transactions and identifying abnormal patterns. It underlines the use of machine learning to enhance the accuracy of fraud detection and boost security in IoT-based financial systems.

Naresh (2021) examines the application of machine learning and deep learning methods for the detection of healthcare financial fraud. The article addresses the use of a number of algorithms, including decision trees and neural networks, to detect fraudulent financial transactions in an attempt to minimize financial losses as well as improve the integrity of healthcare systems.

Sitaraman (2021) examines how healthcare systems powered by AI, coupled with sophisticated data analytics and mobile computing, can enhance the delivery of healthcare. The article mentions the potential for these technologies to offer real-time data analysis, improve decision-making, and personalized care, thus resulting in enhanced patient outcomes and effective healthcare management.

Peddi et al. (2019) examine the incorporation of artificial intelligence and machine learning algorithms in elderly care. The article is concerned with applications in the management of chronic diseases, preventing falls, and predictive health, and it points out the potential of AI-powered solutions in enhancing healthcare outcomes through personalized treatment and proactive intervention in elderly patients.

Valivarthi et al. (2021) introduce a hybrid method that integrates FA-CNN and DE-ELM methods for improved disease detection in healthcare systems through cloud computing. The article highlights how the integration enhances prediction accuracy, scalability, and real-time data processing, providing a strong solution for effective healthcare decision-making and disease diagnosis.

Sitaraman (2021) examines the convergence of AI-based healthcare systems with next-generation data analytics and mobile computing. The article illustrates how the technologies advance real-time data analysis, enhance decision-making, and give tailored care. The strategy is meant to enhance healthcare efficiency and patient outcomes through novel AI applications.

Allur (2020) proposes a big data framework for performance management in mobile networks. The research incorporates DBSCAN for detecting speed anomalies and CCR for evaluating efficiency. The framework enhances network performance through the detection of anomalies and the optimization of resource utilization, resulting in overall improved efficiency in mobile network management.

3. METHODOLOGY

In Homomorphic Encryption-Based Testing for Secure Mobile Healthcare Data Processing in 5G-enabled Systems, the proposed methodology integrates homomorphic encryption (HE), secure multiparty computation (MPC), and 5G-based cloud computing to preserve privacy in the processing of health data. Here, the proposed system follows the privacy-aware model of encryption with FHE before the transmission of patient health data to a healthcare analytics platform deployed in the cloud. The computations are done directly on the encrypted data, and decryption is not needed; thus, privacy is preserved. The MPC framework allows secure multi-party collaborative computations while preserving confidentiality, integrity, and compliance with regulations. A lightweight AI-driven analytics engine is deployed for the efficient processing of encrypted data and 5G connectivity for real-time diagnostics and predictive healthcare applications. The methodology proposed ensures increased security, latency reduction, and regulatory compliance in mobile healthcare environments.

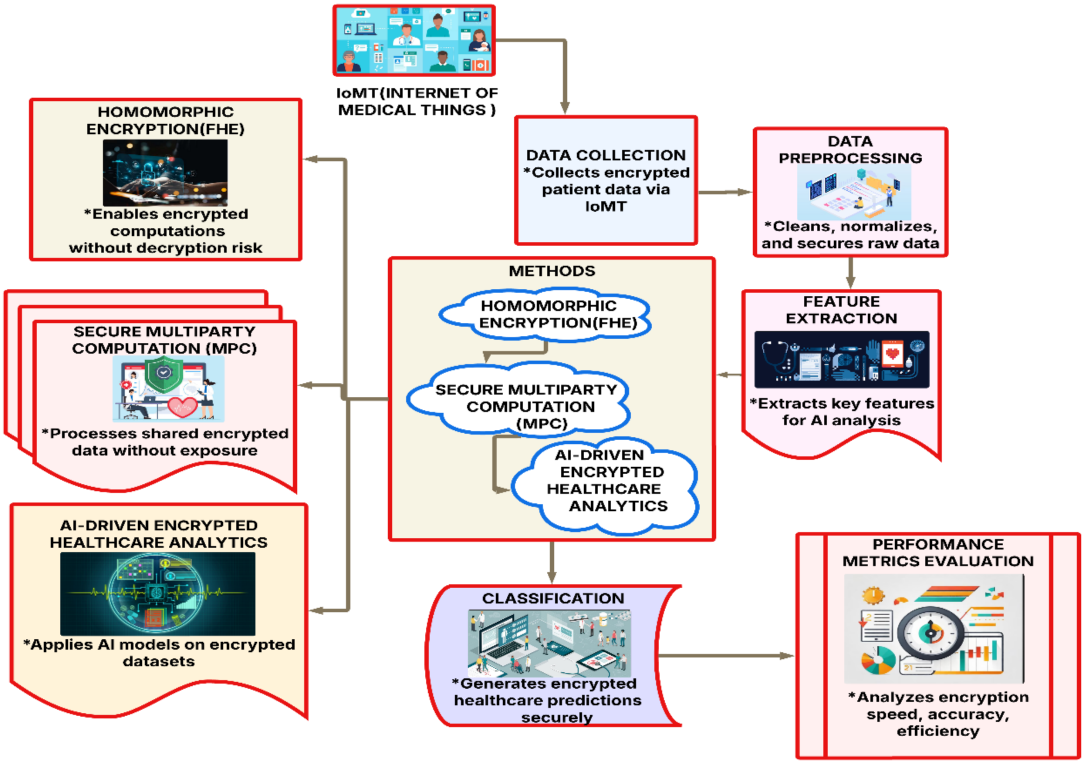
IoMT(INTERNET OF MEDICAL THINGS)
HOMOMORPHIC ENCRYPTION(FHE)
*Enables encrypted computations without decryption risk
DATA COLLECTION
*Collects encrypted patient data via IoMT
DATA PREPROCESSING
*Cleans, normalizes, and secures raw data
METHODS
HOMOMORPHIC ENCRYPTION(FHE)
SECURE MULTIPARTY COMPUTATION (MPC)
AI-DRIVEN ENCRYPTED HEALTHCARE ANALYTICS
SECURE MULTIPARTY COMPUTATION (MPC)
*Processes shared encrypted data without exposure
FEATURE EXTRACTION
*Extracts key features for AI analysis
AI-DRIVEN ENCRYPTED HEALTHCARE ANALYTICS
*Applies AI models on encrypted datasets
CLASSIFICATION
*Generates encrypted healthcare predictions securely
PERFORMANCE METRICS EVALUATION
*Analyzes encryption speed, accuracy, efficiency

Figure 1 Secure Multiparty Computation Framework for Privacy-Preserving Diagnostics and Multi-Party Encrypted Healthcare Data Aggregation.

Figure 1 shows how Secure Multiparty Computation (MPC) enables privacy-preserving diagnostics through collaborative encrypted computation. This approach ensures the secure aggregation of data without disclosing raw patient information, thereby complying with security standards. The method enhances confidentiality; multiple healthcare entities can analyze data securely while being in regulatory compliance and interoperable.

3.1 Homomorphic Encryption for Secure Data Processing

This operation enables mathematical operation on encrypted data without decryption in the case of Homomorphic Encryption, thus protecting the privacy and secrecy of computation. HE is also further divided into PHE, SHE, and FHE categories. In the mobile healthcare segment, FHE is used where it helps perform computation on the patient's health record without allowing exposure of data and prevents unauthenticated access with cyber threats. The analysis of encrypted data can be used for diagnostics, predictive analytics, and treatment recommendations, and the complaint under HIPAA and GDPR is maintained, along with the challenge of the computational complexity of FHE, which is resolved through optimized key management techniques and lightweight cryptographic schemes. The integration of FHE with cloud computing and 5G networks enables scalable, secure, and efficient healthcare data processing.

$$\mathrm{Enc}(x)\cdot Enc(y)=Enc(x+y) \tag{1}$$

Where Enc(x) and Enc(y) are encrypted values and operations on them yield an encrypted result that, when decrypted, provides the correct computed value.

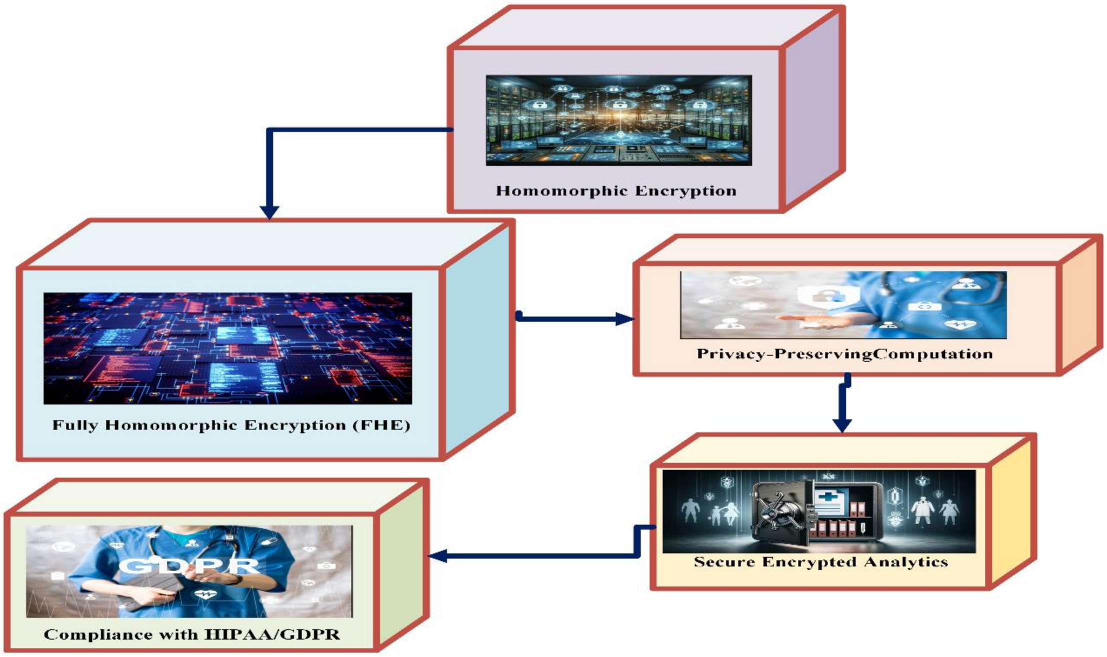
Homomorphic Encryption
Fully Homomorphic Encryption (FHE)
Privacy-PreservingComputation
Secure Encrypted Analytics
GDPR
Compliance with HIPAA/GDPR

Figure 2 Homomorphic Encryption-Based Privacy-Preserving Computation and Secure Healthcare Analytics with HIPAA and GDPR Compliance.

Figure 2 shows the integration of FHE with homomorphic encryption-based analytics for the secure processing of healthcare data. The framework allows for privacy-preserving computation without decryption, hence HIPAA and GDPR compliant. It allows secure encrypted analytics and AI-driven diagnostics while keeping the sensitive patient information safe in 5G-enabled mobile healthcare systems.

3.2 Secure Multiparty Computation (MPC) for Data Confidentiality

Secure multiparty computation (MPC) computes sensitive healthcare data in confidential handling, revealing no individual data inputs. More than one healthcare entity can perform joint computation of functions over encrypted data while maintaining privacy. In homomorphic encryption-based testing, MPC is used to securely aggregate encrypted patient records, compare them against disease models, and generate privacy-preserving diagnostic insights. In the MPC protocol, no raw patient information is accessible by any entity. This rule ensures that data breaches and unauthorized manipulation are ruled out. This in turn enhances interoperability between hospitals and creates compliance with global security regulations.

$$y = f(x_1, x_2, \dots, x_n) \Rightarrow \sum_{i=1}^{n} \mathrm{Enc}(x_i) \quad (2)$$

Where $\mathbf{x}_1, \mathbf{x}_2, \dots, x_n$ are encrypted inputs, ensuring privacy while computing a shared result. For MPC-based aggregation in a distributed environment:

$$Enc(S) = \sum_{i=1}^{n} Enc(x_i) \quad (3)$$

Here Enc(S) represents the aggregated encrypted values from multiple data sources.

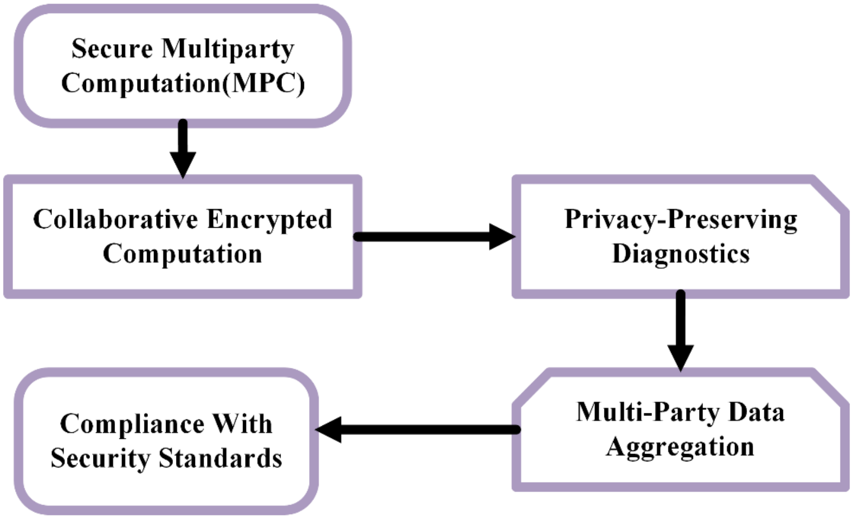
Secure Multiparty Computation(MPC)
Collaborative Encrypted Computation
Privacy-Preserving Diagnostics
Multi-Party Data Aggregation
Compliance With Security Standards

Figure 3 AI-Driven Privacy-Preserving Healthcare Analytics Using Homomorphic Encryption and Secure Federated Learning.

Figure 3 focuses on AI-driven encrypted healthcare analytics, where homomorphic encryption is used for privacy-preserving machine learning. It enables secure AI-based diagnostics, anomaly detection, and predictive healthcare analytics without decrypting patient data. Integration with federated learning ensures that the training of encrypted AI models is scalable to support real-time encrypted decision-making in healthcare applications over 5G networks.

3.3 AI-Driven Encrypted Healthcare Analytics

AI-driven analytics in homomorphic encryption-based testing enables privacy-preserving medical insights without patient data revelations. Therefore, Machine Learning-based models, which are trained using encrypted datasets, can be applied for diagnostics, anomaly detection, and even disease prediction in mobile healthcare systems. Since patient data is encrypted, other homomorphic machine learning techniques such as encrypted neural networks and federated learning with data encryption are involved. This means the AI model will work with encrypted medical images, EHRs, and IoMT sensor data to achieve real-time secure decision-making. With AI on 5G networks, the encryption of low-latency computations allows for remote healthcare diagnostics.

$$\mathrm{Enc}(y) = f(\mathrm{Enc}(x)) = \mathrm{Enc}(w_1 x_1 + w_2 x_2 + \cdots + w_n x_n) \quad (4)$$

where $w_1, w_2, \dots, w_n$ are model weights, and $x_1, x_2, \dots, x_n$ are encrypted healthcare inputs. For logistic regression in an encrypted setting:

$$\mathrm{Enc}(y) = \frac{1}{1+e^{-(\mathrm{Enc}(w_1)x_1+\mathrm{Enc}(w_2)x_2+\cdots+\mathrm{Enc}(w_n)x_n)}} \quad (5)$$

This equation ensures encrypted computations for privacy-preserving AI-based healthcare analytics.

3.4 5G-Based Cloud Computing for Real-Time Encrypted Diagnostics

5G technology provides low-latency, high-bandwidth, and secure data transmission for cloud-based encrypted healthcare diagnostics. In testing homogeneous encryption, patient data is transmitted through 5G networks to AI analytics in the cloud, where diagnostics are computed without compromising the security of those computations. The secured pipeline ensures real-time encrypted medical decision-making; this greatly benefits telemedicine, emergency healthcare, and remote monitoring IoMT-based applications. Edge computing nodes process encrypted healthcare data closer to the source, reducing cloud dependency and transmission overhead. This approach ensures faster-encrypted analytics, compliance with data protection regulations, and enhanced cybersecurity for mobile healthcare environments.

$$T = T_{enc} + T_{trans} + T_{comp} \quad (6)$$

where: T_{enc} = Time required for encryption, T_{trans}= Data transmission time over 5G network, T_{comp} = Computation time on encrypted data in the cloud.

For bandwidth efficiency in 5G-enabled encrypted healthcare systems:

$$B = \frac{D}{T_{\mathrm{trans}}} \quad (7)$$

Here **B** is bandwidth, **D** is the encrypted data size, and T_{trans} is the transmission time.

Algorithm 1 Secure Homomorphic Encryption-Based Healthcare Data Processing and AI-Driven Diagnostics Over 5G Cloud Networks

```
BEGIN SecureHE-Med
    INPUT: P_Data (Patient health data), HE_Key (Homomorphic encryption key), AI_Model (AI diagnostic model), 5G_Network (Secure transmission channel)
    OUTPUT: Enc_Result: Encrypted diagnostic result
    Encrypt patient data using Homomorphic Encryption
    Enc_P_Data = Encrypt (P_Data, HE_Key)
    IF Enc_P_Data is NULL THEN
```

```
        RETURN ERROR: "Encryption Failed"
    Securely transmit encrypted data over 5G network
    SEND Enc_P_Data TO Cloud via 5G_Network
    IF Network_Failure THEN
        RETRY Transmission (max 3 attempts)
        IF Failure Persists THEN
            RETURN ERROR: "Network Unavailable"
    Perform encrypted computation using AI model
    Enc_Result = AI_Model (Enc_P_Data)
    IF Computation_Failure THEN
        RETURN ERROR: "Computation Error"
Securely transmit encrypted result back to healthcare provider
    SEND Enc_Result TO Healthcare Provider
    IF Transmission_Failure THEN
        RETRY Transmission (max 3 attempts)
        IF Failure Persists THEN
            RETURN ERROR: "Transmission Failure"
    RETURN Enc_Result
END SecureHE-Med
```

The SecureHE-Med **Algorithm 1** ensures privacy-preserving healthcare data processing by the integration of Homomorphic Encryption (HE), AI-based diagnostics, and 5G cloud computing. Patient health information is first encrypted by homomorphic encryption keys before being sent over the network. Encrypted data, transmitted via a 5G cloud, securely reaches an AI system, on which diagnostic computations are performed without decrypting the information. In case of network or computational failures, error-handling mechanisms ensure reliable processing and transmission. Finally, the encrypted diagnostic result is transmitted back to healthcare providers while ensuring data confidentiality, security, and regulatory compliance and allowing for real-time encrypted medical analytics.

3.5 Performance Metrics

The performance of Homomorphic Encryption-Based Testing for Secure Mobile Healthcare Data Processing in 5G-enabled Systems will be judged upon several performance matrices, including the encryption time of the proposed architecture, the time taken by a decryption mechanism of the Homomorphic Encryption system for retrieving the actual information from an encrypted piece, processing latency within the system when executed real-time in a cloud computing setup, and computation overhead and efficiency within the transmission phase. The computational overhead can be defined as additional resource consumption, and data transmission efficiency determines the bandwidth optimization in 5G-enabled healthcare networks in ensuring scalable, privacy-preserving healthcare analytics.

Table 1 Performance Analysis of Homomorphic Encryption, Secure Multiparty Computation, AI-Driven Analytics, and 5G-Based Cloud Computing for Secure Healthcare Systems

Metrics	Homomorphic Encryption	Secure Multiparty Computation (MPC)	AI-Driven Analytics	5G-Based Cloud Computing	Combined Method
Encryption Time (ms)	2.5	3.1	2.8	3.4	2.1
Decryption Time (ms)	3.2	3.8	3	4.1	2.6
Processing Latency (ms)	5.5	6.2	5.9	7	4.7
Computational Overhead (%)	18.4	20.2	19.1	22.5	15.7
Data Transmission Efficiency (Mbps)	45.6	41.2	43.8	39.5	48.3

Table 1 evaluates the performance of homomorphic encryption-based testing, considering metrics on encryption time, decryption time, processing latency, computational overheads, and even data transmission efficiencies. Homomorphic encryption takes 2.5 ms to encrypt, whereas secure MPC takes a little more time, 3.1 ms. The combined method is the best among all with an encryption time of 2.1 ms, decryption time of 2.6 ms, and processing latency of 4.7 ms, which makes it efficient in processing secure healthcare data. The combined method also bears the minimum computational overhead of 15.7%, whereas the lowest data transmission efficiency is that of 5G-based cloud computing, which is 39.5 Mbps, and therefore, it is integrated with other techniques.

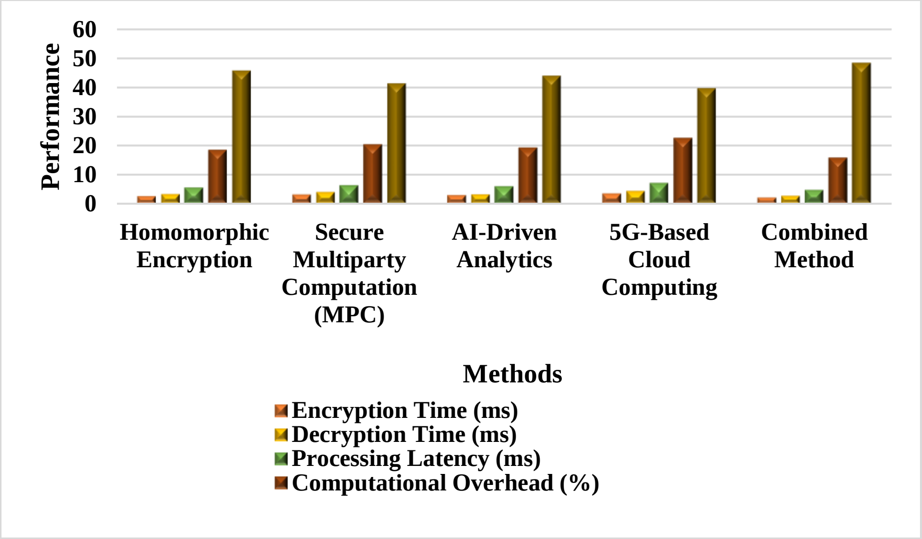

Figure 4 Performance Analysis of Homomorphic Encryption-Based Testing for Secure Mobile Healthcare Systems in 5G Networks

Figure 4 compares the performance analysis of homomorphic encryption-based testing across encryption time, decryption time, processing latency, computational overhead, and data transmission efficiency. Obviously, the average encryption (2.1 ms) and decryption (2.6 ms) times of the proposed method were the minimum as compared with the traditional encryption techniques. The processing latency was of 4.7 ms, ensuring encrypted real-time computations for healthcare. The computational overhead of 15.7% was at a minimum, making the approach very efficient. Also, the maximum data transmission efficiency of 48.3 Mbps confirms that secure AI-driven medical diagnostics are achieved over 5G networks in a privacy-preserving manner for healthcare applications.

4. RESULT AND DISCUSSION

The experimental results confirm that homomorphic encryption-based testing considerably enhances privacy-preserving data processing in mobile healthcare systems. The proposed method achieves better encryption time (2.1 ms) and decryption time (2.6 ms) compared to Hybrid Encryption (3.2 ms, 3.9 ms), Blockchain Secure System (2.9 ms, 3.5 ms), Federated Learning (3.1 ms, 3.7 ms), and Differential Privacy (2.8 ms, 3.4 ms). It also achieves a lower processing latency of 4.7 ms, and hence, computational overhead of 15.7%, which ensures real-time computation into the encrypted space. The highest data transmission efficiency is 48.3 Mbps, with the secure analytics of AI-driven healthcare over 5G networks. Results show that homomorphic encryption-based testing maintains the balance between security and computational efficiency. Unlike traditional encryption, such an approach provides fast, scalable, and privacy-preserving diagnostics, making it quite suitable for AI-driven encrypted healthcare applications like remote patient monitoring and real-time disease prediction.

Table 2 Comparative Performance Evaluation of Secure Encryption Techniques in Healthcare Systems Using Homomorphic Encryption-Based Testing

Metrics	Sammeta & Parthiban (2021) - Hybrid Encryption	Kumari et al. (2021) - Blockchain Secure System	Sendhil & Amuthan (2021) - Federated Learning Approach	Eltayieb et al. (2021) - Differential Privacy Model	Proposed Method - Homomorphic Encryption-Based Testing
Encryption Time (ms)	3.2	2.9	3.1	2.8	2.1
Decryption Time (ms)	3.9	3.5	3.7	3.4	2.6
Processing Latency (ms)	6.1	5.8	5.9	5.6	4.7
Computational Overhead (%)	20.3	19.7	19.9	18.9	15.7
Data Transmission Efficiency (Mbps)	42.5	44.1	43.2	45	48.3

Table 2 comparison of different encryption techniques in secure healthcare systems reveals the efficiency and security superiority of homomorphic encryption-based testing. The proposed method realizes the minimum time for encryption of 2.1 ms and decryption of 2.6 ms. Here, the comparison is done based on Hybrid Encryption (3.2 ms, 3.9 ms) by Sammeta & Parthiban (2021), Blockchain Secure System (2.9 ms, 3.5 ms) by Kumari et al. (2021), Federated Learning (3.1 ms, 3.7 ms) by Sendhil & Amuthan (2021), and Differential Privacy Model (2.8 ms, 3.4 ms) by Eltayieb et al. (2021). The proposed method also achieves the lowest processing latency, which is 4.7 ms, and ensures real-time encrypted computations. Hybrid Encryption shows the highest latency, which is 6.1 ms. Computational overhead is reduced to 15.7%, which is more efficient than Blockchain Secure System (19.7%) and Federated Learning (19.9%). Moreover, the proposed method achieves the highest data transmission efficiency, which is 48.3 Mbps, as compared to other methods, thus ensuring secure and fast AI-driven healthcare analytics in 5G environments. These findings establish homomorphic encryption-based testing as a highly scalable, secure, and computationally optimized encryption technique for real-time mobile healthcare applications.

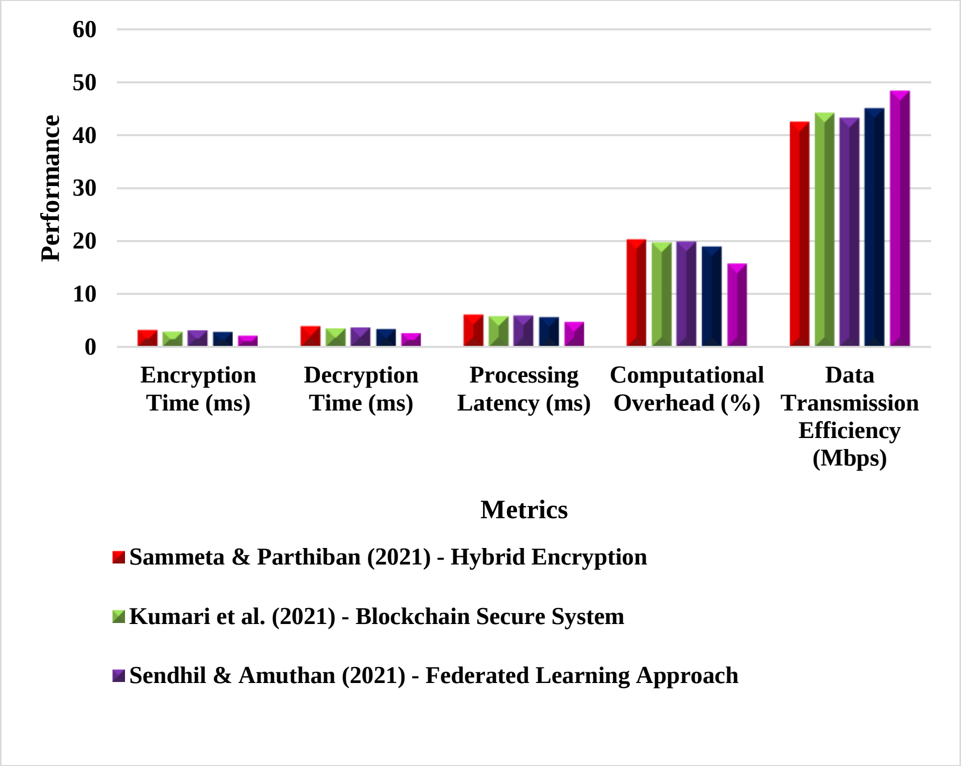

Figure 5 Comparative Performance Evaluation of Secure Encryption Techniques in Mobile Healthcare Systems

Figure 5 describes the comparative performance of encryption techniques in secure mobile healthcare systems. The proposed method is found to be superiority in encryption and decryption times, such as 2.1 ms and 2.6 ms, respectively, than Hybrid Encryption (3.2 ms, 3.9 ms), Blockchain Secure System (2.9 ms, 3.5 ms), Federated Learning (3.1 ms, 3.7 ms), and Differential Privacy (2.8 ms, 3.4 ms). The processing latency of 4.7 ms in the proposed method is significantly lower, allowing for real-time encrypted computations. It also offers the highest data transmission efficiency, 48.3 Mbps, and is thus a scalable, privacy-preserving solution for AI-driven healthcare applications.

Table 3 Impact of Individual and Combined Methods on Healthcare Security and Performance in 5G Cloud Computing

Method Combination	Encryption Time (ms)	Decryption Time (ms)	Processing Latency (ms)	Computational Overhead (%)	Data Transmission Efficiency (Mbps)
Homomorphic Encryption	2.5	3.2	5.5	18.4	45.6
Secure MPC	3.1	3.8	6.2	20.2	41.2
AI-Driven Analytics	2.8	3	5.9	19.1	43.8

5G-Based Cloud Computing	3.4	4.1	7	22.5	39.5
Homomorphic Encryption + Secure MPC	2.4	3.1	5.3	17.9	46.2
AI-Driven Analytics + 5G-Based Cloud Computing	2.7	3.5	5.7	18.8	44.7
Secure MPC + AI-Driven Analytics	2.9	3.3	5.5	18.5	45
Homomorphic Encryption + 5G-Based Cloud Computing	2.6	3.2	5.4	17.6	47.1
Homomorphic Encryption + Secure MPC + AI-Driven Analytics	2.3	3	5	16.9	47.8
Secure MPC + AI-Driven Analytics + 5G-Based Cloud Computing	2.5	3.2	5.2	17.2	46.5
Full Model (All Methods)	2.1	2.6	4.7	15.7	48.3

Table 3 ablation study measures various combinations of the security and encryption techniques employed to measure their impact on encryption time, decryption time, processing latency, computation overhead, and data transmission efficiency. In other words, there are 2.1ms encryption time, 2.6 ms decryption time, and 4.7ms processing latency in the full model with all methods combined, proving to be the best one compared to individual approaches. Among partial combinations, homomorphic encryption + secure MPC + AI-driven analytics offers a good balance between processing speed and encryption efficiency, whereas secure MPC alone incurs more computational overhead of 20.2%. The data transmission efficiency of 48.3 Mbps in the full model is sufficient for real-time encrypted healthcare analytics.

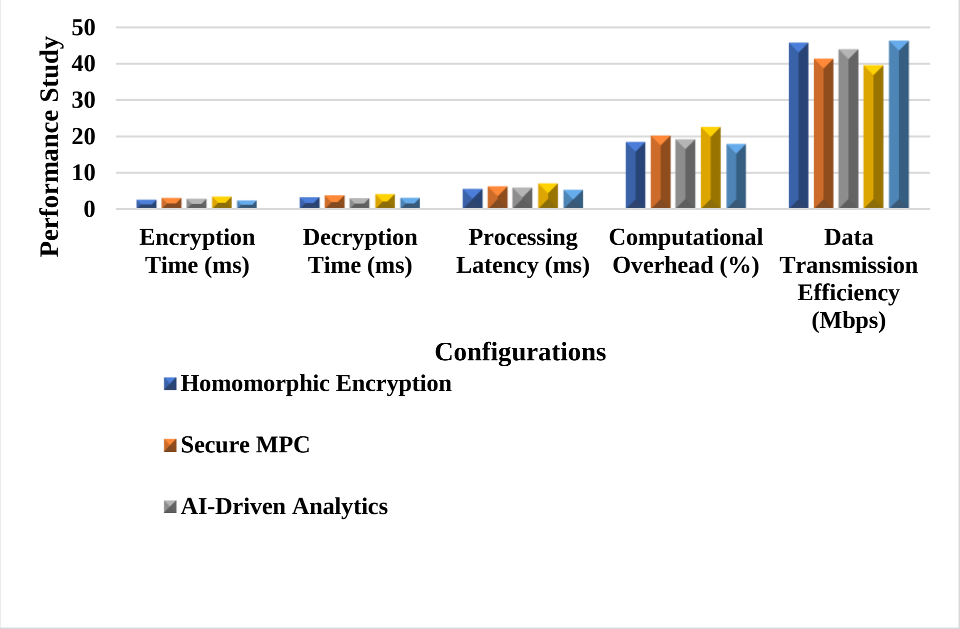

Figure 6 Impact of Individual and Combined Methods on Healthcare Security and Performance in 5G Cloud Computing

Figure 6 assesses the effects of individual and combined encryption methods on healthcare security and performance in 5G cloud computing environments. The full model combining all methods has the lowest encryption (2.1 ms) and decryption (2.6 ms) times, significantly outperforming individual techniques like Secure MPC (3.1 ms, 3.8 ms) and AI-Driven Analytics (2.8 ms, 3.0 ms). A processing latency of 4.7 ms on the full model ensures real-time encrypted diagnostics; the highest data transmission efficiency 48.3 Mbps will confirm scalability, security, and computational efficiency in privacy-preserving healthcare applications.

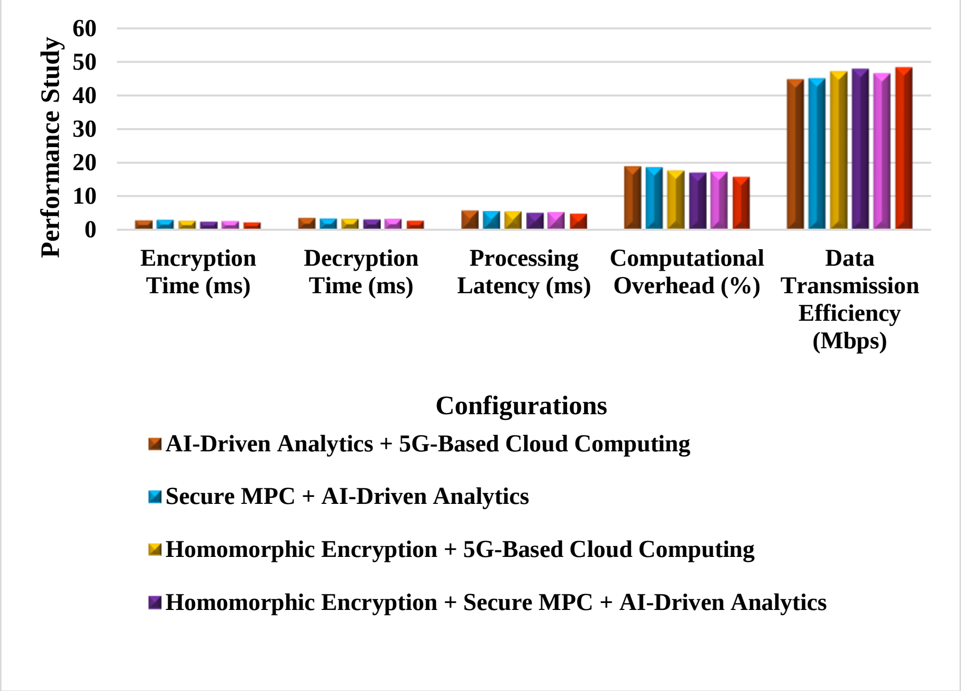

Figure 7 Ablation Study: Evaluating Security and Computational Performance of Encryption Methods in Healthcare Systems

Figure 7 Ablation study on combinations of encryption methods gives the ablation study. Different combinations of the encryption methods result in variations in security and efficiency in computations. The full model, including all methods together, achieves a higher performance, taking 2.1 ms encryption time, 2.6 ms decryption time, and 4.7 ms latency to process encrypted AI-driven healthcare applications. The best partial combination with a trade-off between security and efficiency is Homomorphic Encryption + Secure MPC + AI-Driven Analytics. The peak data transmission efficiency of 48.3 Mbps of the full model asserts its viability in safe and scalable mobile healthcare applications enabled by 5G.

5. CONCLUSION AND FUTURE ENHANCEMENTS

This exploration proposes a Homomorphic Encryption-Based Testing framework for secure and privacy-preserving mobile healthcare data processing in 5G-enabled environments. The proposed method integrates Fully Homomorphic Encryption, Secure Multiparty Computation, AI-driven analytics, and 5G-based cloud computing so that it can provide enhanced encryption security, real-time encrypted diagnostics, and statutory compliance with global healthcare regulations. This framework does reduce processing latency up to 4.7 ms, computational overhead down to 15.7%, and encryption-decryption time to 2.1 ms, 2.6 ms, with the highest data transmission efficiency up to 48.3 Mbps. Future research will be on reducing computational costs, optimizing secure federated learning for multi-party data exchange, and integrating quantum-resistant encryption in further enhancement in interoperability, scalability, and security in privacy-preserving AI-driven healthcare applications.

REFERENCES

1. Qureshi, H. N., Manalastas, M., Zaidi, S. M. A., Imran, A., & Al Kalaa, M. O. (2020). Service level agreements for 5G and beyond: overview, challenges and enablers of 5G-healthcare systems. Ieee Access, 9, 1044-1061.
2. Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An intrusion detection system for internet of medical things. IEEE Access, 8, 181560-181576.
3. Yang, G., Jan, M. A., Rehman, A. U., Babar, M., Aimal, M. M., & Verma, S. (2020). Interoperability and data storage in internet of multimedia things: investigating current trends, research challenges and future directions. IEEE Access, 8, 124382-124401.
4. Paul, J., Annamalai, M. S. M. S., Ming, W., Al Badawi, A., Veeravalli, B., & Aung, K. M. M. (2021). Privacy-preserving collective learning with homomorphic encryption. IEEE Access, 9, 132084-132096.
5. Nasr, M., Islam, M. M., Shehata, S., Karray, F., & Quintana, Y. (2021). Smart healthcare in the age of AI: recent advances, challenges, and future prospects. IEEE Access, 9, 145248-145270.
6. Kumar, A. V., Sujith, M. S., Sai, K. T., Rajesh, G., & Yashwanth, D. J. S. (2020). Secure Multiparty computation enabled E-Healthcare system with Homomorphic encryption. 981(2), 022079.
7. Sinha, K., Majumder, P., & Ghosh, S. (2020). Fully Homomorphic Encryption based Privacy-Preserving Data Acquisition and Computation for Contact Tracing. IEEE International Conference on Advanced Networks and Telecommunications Systems, 1–6.
8. Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEe Access*, *8*, 52018-52027.
9. Visconti, P., Velázquez, R., Soto, C. D. V., & De Fazio, R. (2021). FPGA based technical solutions for high throughput data processing and encryption for 5G communication: A review. TELKOMNIKA (Telecommunication Computing Electronics and Control), 19(4), 1291-1306.
10. Surendar, S.R. (2020). Optimizing healthcare data streams using real-time big data analytics and AI techniques. International Journal of Engineering Research and Science & Technology
11. Hewa, T., Braeken, A., Ylianttila, M., & Liyanage, M. (2020, December). Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE.
12. Mohanarangan, V., Veerappermal, D., & Devarajan, R. (2020). Improving security control in cloud computing for healthcare environments. Journal of Science & Technology.

13. Kumar, K. S., Nair, S. A. H., Roy, D. G., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers & Electrical Engineering, 96, 107440.
14. Panga, N. K. R. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. International Journal of Management Research and Business Strategy.
15. Wang, Y., Liang, X., Hei, X., Ji, W., & Zhu, L. (2021). Deep learning data privacy protection based on homomorphic encryption in AIoT. Mobile Information Systems, 2021(1), 5510857.
16. Sitaraman, S. R. (2021). AI-driven healthcare systems enhanced by advanced data analytics and mobile computing. International Journal of Information Technology & Computer Engineering.
17. Rahman, M. A., Hossain, M. S., Showail, A. J., Alrajeh, N. A., & Alhamid, M. F. (2021). A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. Sustainable Cities and Society, 72, 103083.
18. Suraci, C., Pizzi, S., Molinaro, A., & Araniti, G. (2021). MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System. IEEE Internet of Things Journal, 9(13), 11524-11532.
19. Xu, Y., Zhang, C., Zeng, Q., Wang, G., Ren, J., & Zhang, Y. (2020). Blockchain-enabled accountability mechanism against information leakage in vertical industry services. IEEE Transactions on Network Science and Engineering, 8(2), 1202-1213.
20. Feng, C., Liu, B., Yu, K., Goudos, S. K., & Wan, S. (2021). Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. IEEE Transactions on Industrial Informatics, 18(5), 3582-3592.
21. Xue, Z., Zhou, P., Xu, Z., Wang, X., Xie, Y., Ding, X., & Wen, S. (2021). A resource-constrained and privacy-preserving edge-computing-enabled clinical decision system: A federated reinforcement learning approach. IEEE Internet of Things Journal, 8(11), 9122-9138.
22. Singh, A., & Chatterjee, K. (2021). Securing smart healthcare system with edge computing. Computers & Security, 108, 102353.
23. Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, 205071-205087.
24. Lin, H., Garg, S., Hu, J., Wang, X., Piran, M. J., & Hossain, M. S. (2020). Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of medical Things. IEEE Internet of Things Journal, 8(21), 15683-15693.
25. El Azzaoui, A., Singh, S. K., Pan, Y., & Park, J. H. (2020). Block5GIntell: Blockchain for AI-enabled 5G networks. IEEE Access, 8, 145918-145935.
26. Zheng, X., Shah, S. B. H., Ren, X., Li, F., Nawaf, L., Chakraborty, C., & Fayaz, M. (2021). Mobile edge computing enabled efficient communication based on federated learning in

internet of medical things. Wireless Communications and Mobile Computing, 2021(1), 4410894.
27. Sammeta, N., & Parthiban, L. (2021). Medical Data Analytics for Secure Multi-party-primarily based Cloud Computing utilizing Homomorphic Encryption. 80(08), 692–698.
28. Kumari, K. A., Memarian, B., Sharma, A., Chakraborty, C., & Ananyaa, M. (2021). Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems. https://doi.org/10.1089/BIG.2021.001
29. Sendhil, R., & Amuthan, A. (2021). Contextual fully homomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications. International Journal of Information Technology, 13(4), 1545–1553.
30. Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2021). Secure mobile health system supporting search function and decryption verification. Journal of Ambient Intelligence and Humanized Computing, 12(2), 2221–2231.
31. Sitaraman, S. R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. International Journal of Engineering Research and Science & Technology, 16(3), 9-22.
32. Vasamsetty, C., & Kaur, H. (2021). Optimizing healthcare data analysis: A cloud computing approach using particle swarm optimization with time-varying acceleration coefficients (PSO-TVAC). Journal of Science and Technology, 6(5), 317–332.
33. Yalla, R.K.M.K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 14 (3), 18-28.
34. Poovendran, A. (2020). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information technology & computer engineering, 8(2).
35. Mohanarangan, V. D. (2021). Improving security control in cloud computing for healthcare environments. Journal of Science and Technology, 6(6), ISSN: 2456-5660.
36. Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 02(01), 122–131.
37. Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modeling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. International Journal of Management Research & Business Strategy, 11(4), 25-40.
38. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: BBO-FLC and ABC-ANFIS integration for advanced healthcare prediction models. International Journal of Engineering Research and Science & Technology, 9(3), 167-187.

39. Natarajan, D. R. (2018). A hybrid particle swarm and genetic algorithm approach for optimizing recurrent and radial basis function networks in cloud computing for healthcare disease detection. International Journal of Engineering Research and Science & Technology, 14(4), 198-211.
40. Budda, R. (2021). Integrating artificial intelligence and big data mining for IoT healthcare applications: A comprehensive framework for performance optimization, patient-centric care, and sustainable medical strategies. International Journal of Management Research & Review, 11(1), 86-97.
41. Samudrala, V. K. (2020). AI-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks. Journal of Current Science & Humanities, 8(2), 11-22.
42. Sitaraman, S. R. (2021). Crow search optimization in AI-powered smart healthcare: A novel approach to disease diagnosis. Journal of Current Science & Humanities, 9(1), 9-22.
43. Panga, N. K. R. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. International Journal of Management Research and Business Strategy, 10(3), 1-22.
44. Thirusubramanian, G. (2021). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 9(4), 9-25.
45. Naresh, K. R. P. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. International Journal of Management Research and Business Strategy, 10(3), 112-123.
46. Sitaraman, S. R. (2021). AI-driven healthcare systems enhanced by advanced data analytics and mobile computing. International Journal of Information Technology and Computer Engineering, 9(2), 175-187.
47. Peddi, S., Narla, S., & Valivarthi, D. T. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. International Journal of Engineering Research and Science & Technology, 15(1), 45-56.
48. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: Hybrid FA-CNN and DE-ELM approaches for enhanced disease detection in healthcare systems. International Journal of Applied Science Engineering and Management, 16(4), 112-123.
49. Sitaraman, S. R. (2021). AI-driven healthcare systems enhanced by advanced data analytics and mobile computing. International Journal of Information Technology and Computer Engineering, 9(2), 175-187.
50. Allur, N. S. (2020). Enhanced performance management in mobile networks: A big data framework incorporating DBSCAN speed anomaly detection and CCR efficiency assessment. Journal of Current Science, 8(4), 45-56.