Healthcare Prediction Pipeline using Fully Homomorphic Encryption and GenAI

Prakhar Langer, Gauri Kalnoor, and Y.V. Srinivasa Murthy
School of Computer Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, Karnataka - 575 104, India.
Email IDs: *prakhar.mitblr2022@learner.manipal.edu, gauri.kalnoor@manipal.edu,* and *vishnu.murthy@manipal.edu,*

***Abstract*—Wearable health devices have evolved into powerful tools for continuous monitoring of physiological and behavioral parameters, including heart rate, activity levels, sleep patterns, and caloric expenditure. While these devices enable data-driven healthcare and personalized wellness recommendations, the sensitive nature of the collected information raises significant privacy concerns. This work presents a privacy-preserving health analytics framework that processes wearable data entirely under encryption using the CKKS variant of Fully Homomorphic Encryption (FHE). The system incorporates multiple capabilities: (i) automated ingestion and preprocessing of multimodal wearable datasets, (ii) integration of live, contactless heart rate estimation via remote photoplethysmography (rPPG) from video streams, (iii) secure body mass index (BMI) computation, and (iv) AI-powered personalized health recommendations using a Retrieval-Augmented Generation (RAG) pipeline with a large language model (LLM). Multi-layer authentication — including password verification, device-specific keys, and dynamically generated security challenges — ensures robust access control. All analytics, including anomaly detection and predictive modeling, are performed directly on encrypted data, ensuring confidentiality at every stage. An interactive dashboard visualizes health trends without exposing raw data, enabling users to explore insights securely. By integrating advanced cryptographic techniques with intelligent analytics, the proposed approach demonstrates a scalable pathway toward secure, AI-driven healthcare applications in the wearable technology ecosystem.**

***Index Terms*—Wearable health devices, Privacy-preserving analytics, Fully homomorphic encryption, CKKS scheme, Remote photoplethysmography, BMI estimation, Anomaly detection, Retrieval-augmented generation, Large language models, Secure healthcare systems.**

I. Introduction

Over the past decade, wearable health technology has evolved from simple pedometers into sophisticated multi-sensor systems capable of continuous physiological and behavioral monitoring. Modern wearable devices—including smartwatches, fitness trackers, smart clothing, and head-mounted sensors—can record a broad range of parameters such as heart rate, step count, activity intensity, sleep cycles, respiration rate, and even peripheral oxygen saturation. These data streams, collected at high temporal resolution, have unlocked unprecedented opportunities for personalized healthcare, early detection of health risks, and the development of data-driven wellness interventions.

The integration of wearable data into healthcare workflows enables clinicians and individuals alike to make informed, real-time decisions about activity planning, recovery, nutrition, and lifestyle optimization. Population-level analysis of aggregated wearable data can also reveal trends in physical activity, detect anomalies indicative of community-level health changes, and contribute to predictive models for chronic disease management. In parallel, advances in machine learning (ML) and artificial intelligence (AI) have enabled more complex pattern recognition, risk stratification, and adaptive recommendation systems that leverage wearable sensor data for individualized insights.

Despite these advantages, the sensitive nature of wearable health data poses significant privacy and security challenges. These datasets contain detailed, personally identifiable information (PII) that can be exploited if improperly accessed, including health status, daily routines, and behavioral patterns. Unauthorized access, malicious misuse, or unintentional disclosure of such data can lead to severe consequences, including identity theft, health-based discrimination, targeted marketing exploitation, or denial of insurance benefits. Traditional data analytics architectures for wearables often rely on centralized cloud-based processing pipelines. In most cases, these require decrypting raw data before computation, creating a vulnerable exposure window where sensitive information may be intercepted or compromised. This exposure risk is further amplified when processing is outsourced to third-party AI providers or cloud services.

Addressing this challenge requires computation paradigms that can preserve data confidentiality throughout the analytics lifecycle. Fully Homomorphic Encryption (FHE) is an emerging cryptographic technique that allows mathematical operations to be performed directly on encrypted data, producing encrypted outputs that can be decrypted only by the data owner. In contrast to conventional encryption schemes, FHE ensures that at no stage—during storage, transmission, or computa-

tion—does the plaintext data need to be revealed. This property makes FHE particularly attractive for health analytics, where sensitive physiological signals can be processed without compromising privacy. The CKKS variant of FHE is especially suited for wearable health applications, as it supports approximate arithmetic over real-valued data, enabling the execution of statistical calculations, anomaly detection, and ML inference tasks directly on ciphertext.

In this work, we present an end-to-end privacy-preserving health analytics platform that leverages FHE to secure multi-modal wearable data from acquisition to visualization. The system is designed to ingest raw data streams from heterogeneous wearable devices, perform preprocessing and feature engineering, and enrich the dataset with additional metrics such as live heart rate estimation from remote photoplethysmography (rPPG) via webcam input and body mass index (BMI) computation from user-provided anthropometric data. Immediately after preprocessing, all features are encrypted using CKKS-based FHE and remain encrypted throughout subsequent processing stages, including statistical summarization, predictive modeling, and anomaly detection. This design ensures that neither intermediate results nor raw measurements are ever exposed to untrusted environments.

To complement privacy-preserving analytics, the platform incorporates an AI-driven recommendation engine based on a large language model (LLM) operating within a Retrieval-Augmented Generation (RAG) framework. This approach grounds the LLM's responses in relevant, curated health knowledge, enabling the generation of personalized, context-aware recommendations without exposing user data to external AI services in plaintext form.

Security is further reinforced through a multi-layer authentication mechanism that combines traditional password verification, a device-specific cryptographic key, and dynamically generated security questions to mitigate the risk of credential compromise. The output of the analytics pipeline is delivered via an interactive, web-based dashboard that allows users to explore trends, correlations, and predictive insights in an encrypted-safe visualization environment. This ensures that the privacy guarantees of the system extend all the way to the user interface.

The main contributions of this work are as follows:

- **A generalized privacy-preserving analytics framework** for multi-modal wearable health data, built on CKKS-based FHE to enable computation on encrypted data without decryption.
- **A secure multi-layer authentication protocol** integrating conventional credentials with device-specific keys and dynamically generated security challenges.
- **An AI-driven personalized health guidance module** utilizing LLMs in a RAG configuration to produce contextually relevant recommendations while preserving data privacy.
- **A privacy-respecting visualization dashboard** for interactive exploration of health metrics and model predictions without revealing raw personal information.

By integrating advanced cryptographic computation with intelligent, AI-driven analytics, this platform demonstrates that it is possible to achieve high-utility wearable health insights without compromising user privacy. The proposed framework offers a scalable foundation for secure, trustworthy healthcare systems in an era of ubiquitous sensing and AI-powered decision support.

II. Literature Review

The convergence of wearable sensing, artificial intelligence, and advanced cryptography has led to significant progress in secure health analytics. Existing literature provides a strong foundation for privacy-preserving computation in healthcare, but several gaps remain when applying these methods to multi-modal wearable data and real-time personalized recommendations. Homomorphic encryption has emerged as a promising approach for secure computation in sensitive domains such as medicine and bioinformatics. Wood et al. [1] provide a comprehensive overview of HE techniques for medical machine learning, highlighting the suitability of schemes like CKKS for real-valued biomedical data. Similarly, Gandhi et al. [2] propose collaborative learning frameworks that employ HE to protect patient privacy while enabling cross-institutional analytics. Babu et al. [3] extend this concept to decentralized machine learning in healthcare, demonstrating how FHE can secure distributed training across multiple centers without exposing raw data. Specific disease-focused implementations, such as confidential classifiers [4] and privacy-preserving heart disease prediction models [5], illustrate the potential of HE for specialized clinical use cases.

While these studies confirm the feasibility of HE in healthcare, most focus on structured clinical datasets or specific prediction tasks. In contrast, the proposed work targets multi-modal wearable data, which introduces higher variability, real-time processing needs, and integration challenges with live biometric signals such as rPPG-derived heart rate. Beyond encryption, privacy-preserving machine learning (PPML) has been widely studied in the healthcare domain. Guerra-Manzanares et al. [6] outline open challenges in deploying PPML, emphasizing computational overhead, model accuracy under encryption, and integration with clinical workflows.

Reviews by Naresh et al. [7] and Sasirekha et al. [8] consolidate techniques including differential privacy, federated learning, and secure multiparty computation. Wang et al. [9] propose user-centric data sharing frameworks that allow patient-controlled privacy policies. However, these works often lack integration with consumer-grade wearable devices, where data originates from multiple sensor modalities and may require continuous processing. Our approach builds upon these findings by coupling CKKS-based FHE with streaming data ingestion, ensuring that both stored and real-time wearable data remain encrypted throughout all computational stages. Recent advances in large language models (LLMs) have opened new opportunities for clinical decision support, education, and healthcare administration [10]. Studies have explored hybrid systems where human expertise complements LLM-driven recommendations [11], as well as evaluations of LLM performance in clinical workflows [12], [13]. Oniani et al. [14] demonstrate the potential of grounding LLMs with clinical practice guidelines to improve reliability in decision-making. However, most LLM-based healthcare applications rely on unencrypted patient data, creating potential privacy risks. The proposed framework addresses this gap by embedding the LLM within a Retrieval-Augmented Generation (RAG) pipeline, ensuring that only encrypted intermediate features and privacy-preserving retrieval results are used in generating personalized recommendations. Encrypted model inference has seen rapid development, with methods for secure execution of vision models [15], encrypted melanoma detection [16], and parallel secure inference across multiple models using CKKS [17]. Gamba [18] discusses the trade-offs between accuracy and speed in homomorphic inference, while Chen et al. [19] address multicenter inference scenarios in medical imaging. Despite these advancements, few works have explored encrypted inference pipelines tailored to wearable data analytics, which often involve a combination of statistical calculations, anomaly detection, and ML predictions. While prior studies have demonstrated the viability of FHE and PPML in healthcare, most have been applied to static datasets or specialized medical imaging tasks. Large language model integration has largely been explored without privacy-preserving computation, and wearable health data—especially when enriched with live biometric signals—remains underrepresented in secure analytics research.

The proposed system bridges these gaps by:

- Applying CKKS-based FHE to continuous, multimodal wearable data streams, including live rPPG heart rate signals.
- Combining encrypted computation with AI-driven personalized recommendations via a privacy-preserving RAG-LLM pipeline.
- Introducing a multi-layer authentication mechanism to safeguard access in consumer and clinical contexts.
- Delivering privacy-preserving insights through an interactive dashboard that never exposes raw data.

This integration of advanced cryptographic computation, real-time biometric analytics, and AI-driven personalization represents a novel contribution to the wearable healthcare privacy landscape.

III. Proposed Methodology

The proposed system follows a modular pipeline that ensures privacy preservation, secure access control, and intelligent health analytics from wearable device data. The core stages are illustrated in the system architecture and described below.

A. Data Acquisition and Preprocessing

The pipeline begins with the secure upload of raw wearable data exports. These datasets typically contain multi-modal measurements such as daily step counts, heart rate, calories burned, and sleep metrics. Upon ingestion, the files are automatically extracted, merged, and reformatted into a unified data structure. Preprocessing involves:

- Standardizing timestamps across all data sources.
- Removing duplicate or inconsistent records.
- Handling missing values using appropriate imputation strategies.
- Generating derived features such as *sleep quality* (ratio of minutes asleep to total time in bed), goal achievement flags, activity intensity ratios, and body mass index (BMI) from user-provided attributes.

B. Anomaly Detection

Given the noise-prone nature of physiological sensor data, an anomaly detection module identifies irregular or corrupted readings. This is achieved by:

- Aggregating heart rate readings into minute-level averages.
- Normalizing the values for scale consistency.
- Applying an Isolation Forest model to flag outlier points, which are then labeled as potential anomalies.

These anomaly indicators are later integrated into trend analysis and visualization, helping to highlight irregular health events without compromising data integrity.

C. Privacy-Preserving Computation with FHE

To ensure that sensitive personal data is never exposed in plaintext during processing, the system employs the *CKKS* variant of Fully Homomorphic Encryption (FHE). This scheme allows approximate mathematical operations on encrypted real-valued data, making it well-suited for health analytics tasks. The key steps are:

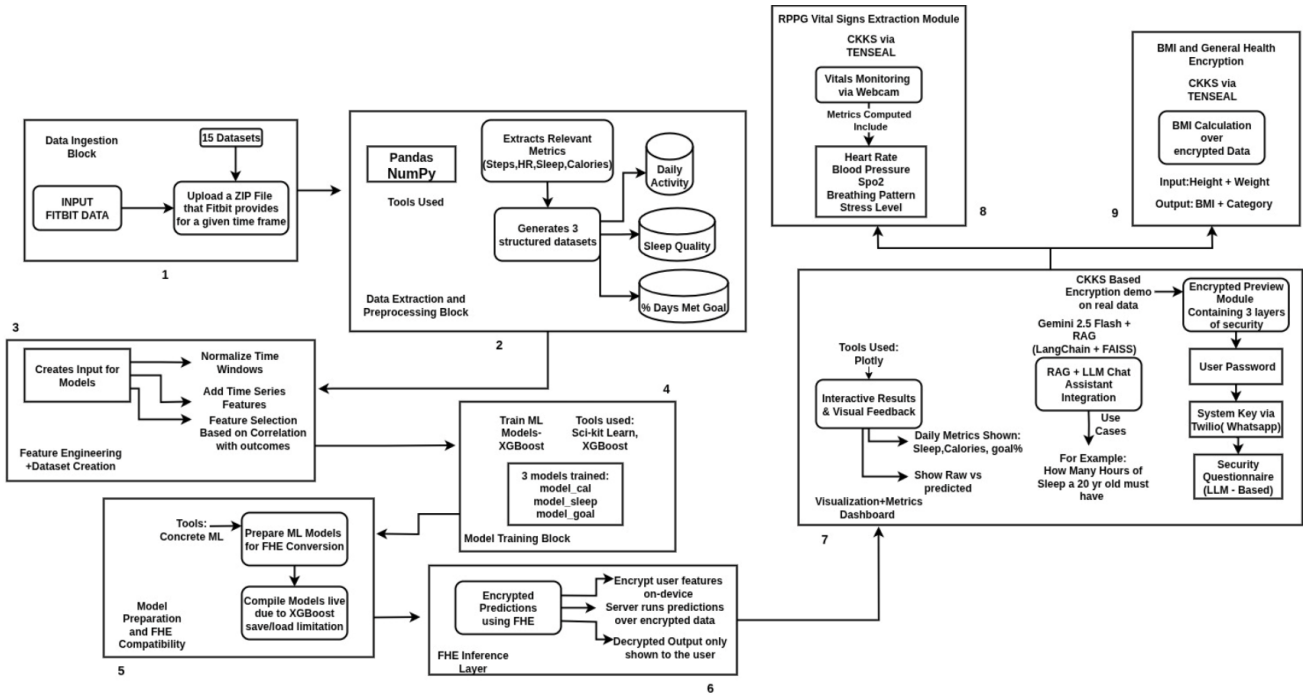

Fig. 1. Proposed system architecture for privacy-preserving wearable health analytics.

- Encrypting the processed feature vectors on the client side before any server-based computation.
- Running machine learning inference directly on ciphertexts, with no decryption occurring on the server.
- Returning encrypted predictions to the client, where they are decrypted for presentation.

This guarantees that neither intermediate results nor final analytics are visible to the processing environment, enabling secure outsourcing of computation.

D. Predictive Modeling

The encrypted data serves as input to pre-trained predictive models:

- **Calorie Prediction:** XGBoost regressor estimates daily caloric expenditure based on activity and physiological features.
- **Sleep Quality Prediction:** Another regressor forecasts expected sleep quality given user habits and biometric signals.
- **Goal Achievement Classification:** An XGBoost classifier predicts whether the daily activity goal is likely to be met.

These models are trained offline in an FHE-compatible format so that their inference steps can be executed on encrypted data without modification.

E. Multi-Layer Authentication

To further safeguard access, the system implements a three-stage authentication mechanism:

1) **Password Verification:** Traditional credential matching for initial identity validation.
2) **Device-Specific Key:** A unique, time-sensitive key provided to the user during login.
3) **Dynamic Security Question:** A randomly selected challenge generated from pre-stored personal facts, ensuring resistance to static credential attacks.

Only users passing all three stages can proceed to encrypted analytics and personalized dashboard access.

F. AI-Driven Health Recommendations

The final stage integrates an *LLM*-powered recommendation engine using a Retrieval-Augmented Generation (RAG) framework. The process:

1) Retrieves relevant health knowledge from a curated knowledge base.
2) Combines this with the user's encrypted-and-processed analytics.
3) Generates personalized, context-aware recommendations in natural language.

This approach ensures that insights are not generic but tailored to the individual's data trends.

IV. Results and Observations

When tested with real wearable device exports, the system executed the complete workflow as follows:

A. Secure Login and Data Upload

The user successfully authenticated through all three security layers. Upon upload, the platform automatically extracted the relevant CSV files, merged them into a consistent dataset, and calculated all derived metrics.

B. Encryption Demonstration

Before analysis, the preprocessed data was encrypted locally using CKKS. An encryption preview module allowed the user to see both the plaintext and its encrypted form, alongside a test computation (e.g., doubling values under encryption) to confirm the correctness of encrypted operations.

C. Encrypted Analytics

The encrypted feature vectors were passed to the pretrained XGBoost models. The server produced encrypted predictions for calories, sleep quality, and goal achievement status. These predictions were decrypted on the client side and presented in tabular form next to actual recorded values, enabling side-by-side comparison.

D. Anomaly Insights

Heart rate readings flagged as anomalies by the Isolation Forest model were highlighted in the results, allowing the user to visually identify unusual physiological patterns.

E. Interactive Dashboard

The Streamlit-based dashboard displayed:

- Daily trends for calories, sleep quality, and activity goals.
- Summary statistics such as average calorie burn and proportion of days meeting goals.
- Correlation and trend charts that provide deeper insight into health patterns.

Importantly, these visualizations were generated without exposing raw sensitive values on the server.

F. Personalized AI Recommendations

The user could query the integrated chatbot for advice on improving health metrics. Responses reflected both the user's data patterns and relevant medical guidelines retrieved by the RAG pipeline, delivering actionable and privacy-respecting guidance.

In conclusion, the results demonstrate that the system operates as a fully functional privacy-preserving health analytics platform — from multi-modal data ingestion to encrypted computation, secure visualization, and AI-driven personalization — without ever revealing raw health data at any processing stage.

References

[1] Alexander Wood, Kayvan Najarian, and Delaram Kahrobaei. Homomorphic encryption for machine learning in medicine and bioinformatics. *ACM Computing Surveys (CSUR)*, 53(4):1–35, 2020.

[2] Bhomik M Gandhi, Shruti B Vaghadia, Malaram Kumhar, Rajesh Gupta, Nilesh Kumar Jadav, Jitendra Bhatia, Sudeep Tanwar, and Abdulatif Alabdulatif. Homomorphic encryption and collaborative machine learning for secure healthcare analytics. *Security and Privacy*, 8(1):e460, 2025.

[3] Kattinti Mahesh Babu, Meharaz Syed, Shajoon Shaik, Sarala Thalari, Umamaheswari Macha, and Anusha Chatakondu. Fully homomorphic encryption framework for privacy preserving in healthcare through decentralized machine learning. In *Challenges in Information, Communication and Computing Technology*, pages 812–816. CRC Press, 2025.

[4] Aditya Malik, Nalini Ratha, Bharat Yalavarthi, Tilak Sharma, Arjun Kaushik, and Charanjit Jutla. Confidential and protected disease classifier using fully homomorphic encryption. In *2024 IEEE Conference on Artificial Intelligence (CAI)*, pages 365–370. IEEE, 2024.

[5] Vankamamidi S Naresh and Sivaranjani Reddi. Exploring the future of privacy-preserving heart disease prediction: a fully homomorphic encryption-driven logistic regression approach. *Journal of Big Data*, 12(1):52, 2025.

[6] Alejandro Guerra-Manzanares, L Julian Lechuga Lopez, Michail Maniatakos, and Farah E Shamout. Privacy-preserving machine learning for healthcare: open challenges and future perspectives. In *International Workshop on Trustworthy Machine Learning for Healthcare*, pages 25–40. Springer, 2023.

[7] Vankamamidi S Naresh and Muthusamy Thamarai. Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 13(2):e1490, 2023.

[8] B Sasirekha and C Gunavathi. Systematic review on privacy-preserving machine learning techniques for healthcare data. *Journal of Cyber Security Technology*, pages 1–26, 2025.

[9] Lianhai Wang, Lingyun Meng, Fengkai Liu, Wei Shao, Kunlun Fu, Shujiang Xu, and Shuhui Zhang. A user-centered medical data sharing scheme for privacy-preserving machine learning. *Security and Communication Networks*, 2022(1):3670107, 2022.

[10] Josip Vrdoljak, Zvonimir Boban, Marino Vilović, Marko Kumrić, and Joško Božić. A review of large language models in medical education, clinical decision support, and healthcare administration. In *Healthcare*, volume 13, page 603. MDPI, 2025.

[11] Elena Sblendorio, Vincenzo Dentamaro, Alessio Lo Cascio, Francesco Germini, Michela Piredda, and Giancarlo Cicolini. Integrating human expertise & automated methods for a dynamic and multi-parametric evaluation of large language models' feasibility in clinical decision-making. *International Journal of Medical Informatics*, 188:105501, 2024.

[12] Solène Delourme, Akram Redjdal, Jacques Bouaud, and Brigitte Seroussi. Measured performance and healthcare professional perception of large language models used as clinical decision support systems: a scoping review. *Studies in health technology and informatics*, 316:841–845, 2024.

[13] Paul Hager, Friederike Jungmann, Robbie Holland, Kunal Bhagat, Inga Hubrecht, Manuel Knauer, Jakob Vielhauer, Marcus Makowski, Rickmer Braren, Georgios Kaissis, et al. Evaluation and mitigation of the limitations of large language models in clinical decision-making. *Nature medicine*, 30(9):2613–2622, 2024.

[14] David Oniani, Xizhi Wu, Shyam Visweswaran, Sumit Kapoor, Shravan Kooragayalu, Katelyn Polanska, and Yanshan Wang. Enhancing large language models for clinical decision support by incorporating clinical practice guidelines. In *2024 IEEE 12th International Conference on Healthcare Informatics (ICHI)*, pages 694–702. IEEE, 2024.

[15] Jia-Lin Chan, Wun-She Yap, C-K Denis, Bok-Min Goi, and Wai-Kong Lee. Privacy-preserving detection of helmet and mask

wearing with fully homomorphic encryption: Towards a secure inference approach. In *2024 IEEE 8th Forum on Research and Technologies for Society and Industry Innovation (RTSI)*, pages 554–559. IEEE, 2024.

[16] Nayna Jain, Karthik Nandakumar, Nalini Ratha, Sharath Pankanti, and Uttam Kumar. Cryptinfer: Enabling encrypted inference on skin lesion images for melanoma detection. In *Proceedings of the First International Conference on AI-ML Systems*, pages 1–7, 2021.

[17] Weibin Wu, Ying Wang, Yangpan Zhang, Luyao Wang, and Lu Zhou. Parallel secure inference for multiple models based on ckks. In *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data*, pages 199–213. Springer, 2024.

[18] Matteo Gamba. Privacy-preserving inference with homomorphic cryptography: Challenges and modern approaches for fast and accurate two-parties private inference, 2024.

[19] Jingwei Chen, Chen Yang, Yuwen Chen, Kunhua Zhong, Wenqiang Yang, Jiang Liu, Wenyuan Wu, and Bin Yi. Secure multicenter medical model inference from homomorphic encryption. In *International Conference on Intelligent Computing*, pages 135–147. Springer, 2025.