A Hybrid Homomorphic and Functional Encryption Prototype for Secure Medical Data Processing in Cloud Environments

Jack Leacock, Kevin Curran, Pratheepan Yogarajah

Ulster University, Northern Ireland

Abstract

The secure utilisation of highly sensitive data—such as clinical records or personal and business banking information—remains a critical unresolved challenge in modern digital infrastructure. Organisations increasingly rely on cloud-based analytics, yet conventional security models require decryption prior to processing, exposing data to breaches, insider threats, and cross-domain misuse. Existing access-control frameworks further depend on trusted server-side enforcement, offering limited guarantees once decryption keys are released.

This research proposes a fully integrated Hybrid Functional Encryption (FE) and Homomorphic Encryption (HE) system designed to enable secure, policy-governed computation over encrypted data stored entirely in untrusted environments. In the envisioned completed system, raw data—whether patient vitals or financial transactions—are encrypted client-side using HE, enabling servers to perform analytics such as trend detection, risk scoring, or cohort aggregation *without ever revealing plaintext*. Decryption capabilities are controlled through a rigorous FE-based mechanism in which users receive function-specific keys bound to explicit, expressive policies defined over roles, attributes, intent, and contextual factors. This ensures that even authorised users gain access only to permitted outputs—never the underlying raw data.

The final system will support large-scale ingestion pipelines, multi-tenant cloud storage, distributed policy-evaluation services, and secure computation endpoints capable of processing thousands of encrypted records in real time. A unified audit and performance-tracking layer will quantify scalability, key-distribution efficiency, and computational overheads across clinical and financial datasets.

By combining HE-based encrypted computation with FE-governed, mathematically enforced access control, this work aims to deliver a robust, generalisable architecture for privacy-preserving analytics across healthcare, finance, and other data-sensitive sectors, offering a path toward zero-trust, regulation-compliant data processing in cloud-native environments.