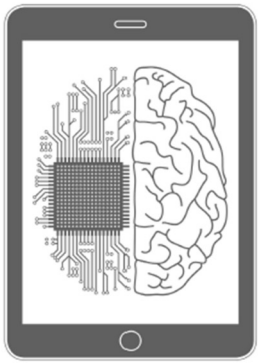
University of Applied Sciences and Arts Northwestern Switzerland
School of Life Sciences

Fully Homomorphic Encryption for Data Privacy in Personal Genotype Reports



Massaro Gabriel
Master-Thesis

Supervisor: Dr. Pascal Moriggl, FHNW
Expert: Dr. Quy Vo-Reinhard, dHealth Foundation

Problem Statement

Privacy and Security Concerns:
With healthcare's growing dependency on cloud computing, significant data privacy and security issues emerge, particularly for sensitive genomic data used in diagnostics and research.

Direct-to-Consumer (DTC) Genetic Reports:
The popularity of DTC genetic testing platforms, like 23andMe, has allowed access to personal genomic information. These reports also pose a risk of unauthorized access and misuse of sensitive genetic data.

Ethical and Technical Challenges:
Ensuring data security and privacy in genomic research involves both ethical concerns and overcoming technical barriers.

Methodology

Design Research Approach:
The design research methodology was used, focusing on developing and evaluating a prototype for secure genomic data processing

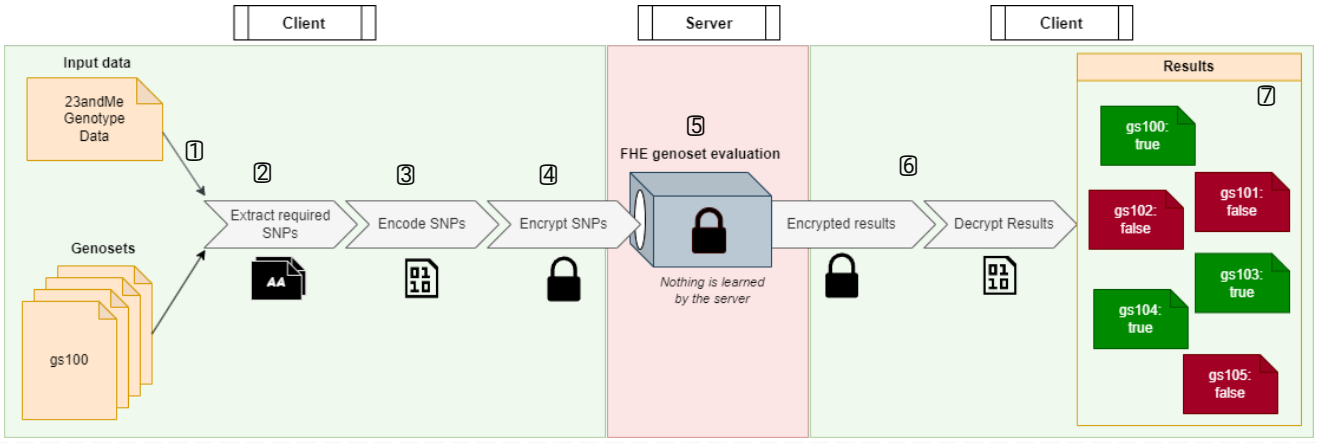
Fully Homomorphic Encryption (FHE):
The potential of FHE was explored to enable secure computations on encrypted data, maintaining privacy without the need for decryption.

Prototype Development and Testing:
A prototype was created in the Rust programming language to demonstrate the feasibility and performance of FHE in evaluating encrypted genotype data.

Solution

This solution makes use of **Fully Homomorphic Encryption (FHE)** and is designed to maintain the confidentiality of sensitive genetic information:

1 Initially, the client (patient) inputs their 23andMe genotype data, from which specific genetic markers called SNPs are 2 extracted, 3 encoded, and then 4 FHE encrypted. 5 These encrypted SNPs are sent to a server (third-party analysis server) where an FHE genoset evaluation is performed without the server learning any underlying genetic information. 6 The server sends the encrypted results back to the client, where they are decrypted, 7 revealing the result of certain genosets (gs100, gs101, etc.) as true or false. The client's genetic data remains confidential throughout the process.



Results

Effective Privacy Preservation:
The prototype effectively secured genomic data. Allowing true end-to-end security (during transit, storage, and **computation**).

Computational Efficiency:
With FHE genoset evaluation being only **5-10 times** slower than cleartext evaluation, the prototype showed adequate performance.

Accuracy:
The solution achieved a **100%** accuracy (match rate) in the output comparison between FHE and the cleartext results.

Security:
The prototype, with an estimated 128-bit security, is secure against post-quantum attacks.

Conclusion

FHE's Role in Healthcare Data Security:
The thesis confirms FHE's capability to enhance privacy and security in processing sensitive genomic data.

Main Contributions:
Highlights the successful application of FHE in securing personal genomic data, offering a promising solution for privacy-preserving data analysis.

Future Directions:
Suggests further development of FHE systems to meet the growing demand for secure genomic data processing, emphasizing the need for improved computational efficiency.