Privacy-Preserving Artificial Intelligence: Application to Precision Medicine

Anamaria Vizitiu, Cosmin Ioan Niță, Lucian Mihai Itu

Transilvania University of Brasov, Brasov, Romania

Universitatea Transilvania din Brașov

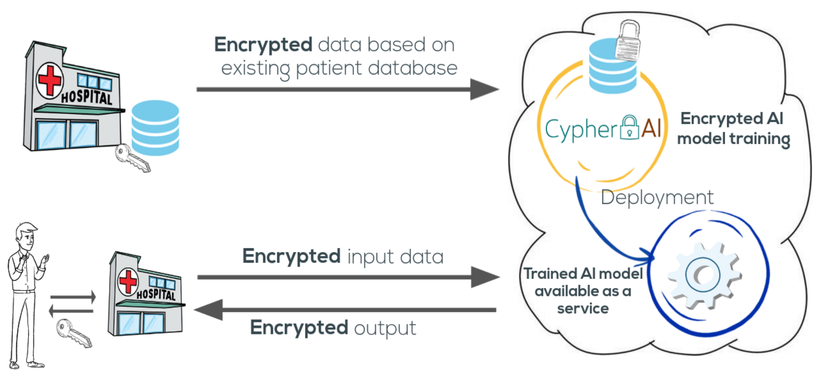
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732907

Introduction

Despite the potential of Machine Learning in **enabling personalized medicine application,** the adoption of Deep Learning based solutions in clinical workflows has been hindered in many cases by the strict regulations concerning the **privacy of patient health data**. To address this vulnerability, we adapt current Deep learning (DL) algorithms to **handle only encrypted data** using homomorphic encryption (HE).

Methods

The secure processing of medical data is performed in such a way that the external party cannot derive knowledge from the data, and the user is unable to obtain information regarding the machine learning model.



HOMOMORPHIC ENCRYPTION

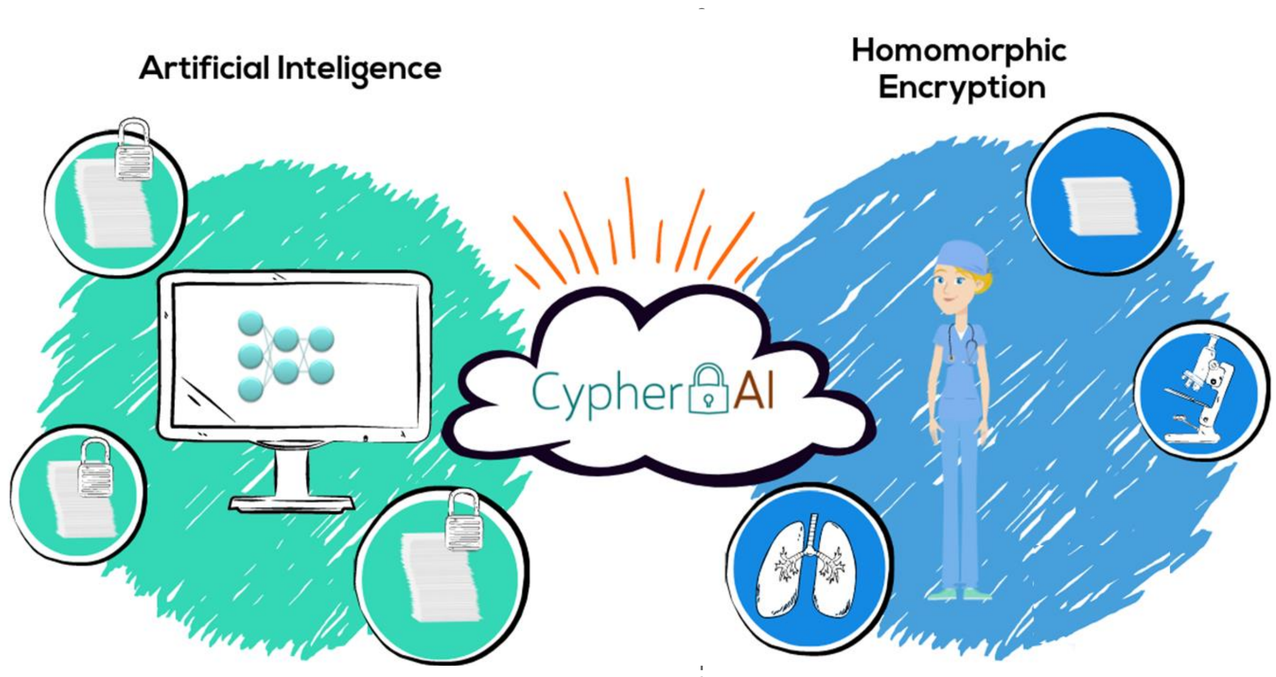
Homomorphic encryption (HE) is a form of encryption that allows computation directly on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

THE MORE ENCRYPTION SCHEME

- Homomorphic w.r.t. algebraic operations, and certain non-linear operations (exponential, logarithmic, square root)
- Operates directly on rational numbers
- Tradeoffs in security.

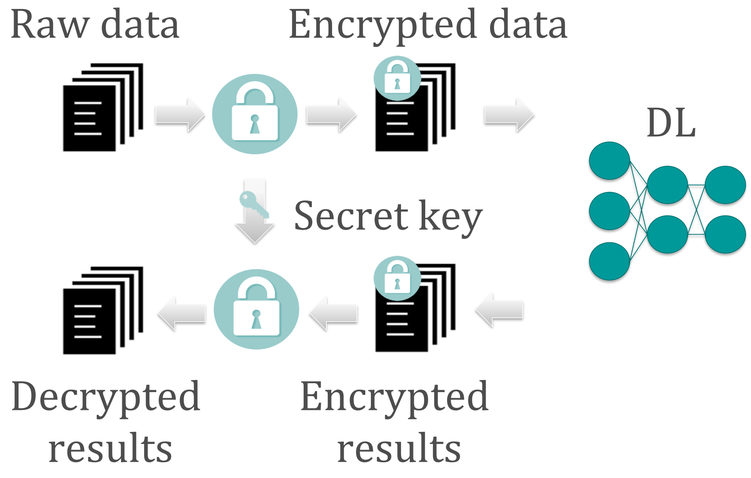
The MORE [1] scheme relies on matrix algebra and encrypts a numerical value as a matrix.

[1] Kipnis, Aviad and Eliphaz Hibshoosh. "Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification." *IACR Cryptology ePrint Archive* 2012 (2012): 637.



Artificial Intelligence and Homomorphically Encrypted Data

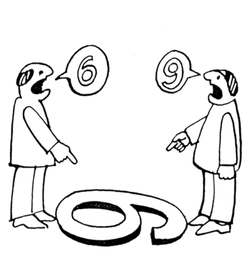
Deep Learning (DL) based solutions can be developed using homomorphically encrypted input-output data



USE CASES

To evaluate the use of Deep Neural Networks models over encrypted data 3 use cases were addressed.

A



B

C

Results

Numerical differences between the results of unencrypted and encrypted models are negligible, with the computation time being one order of magnitude slower for the encrypted cases.

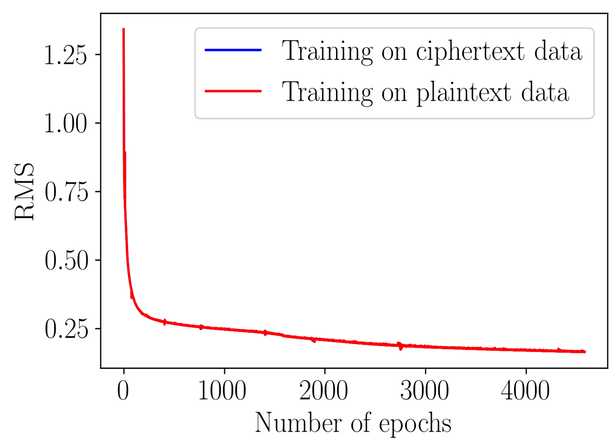
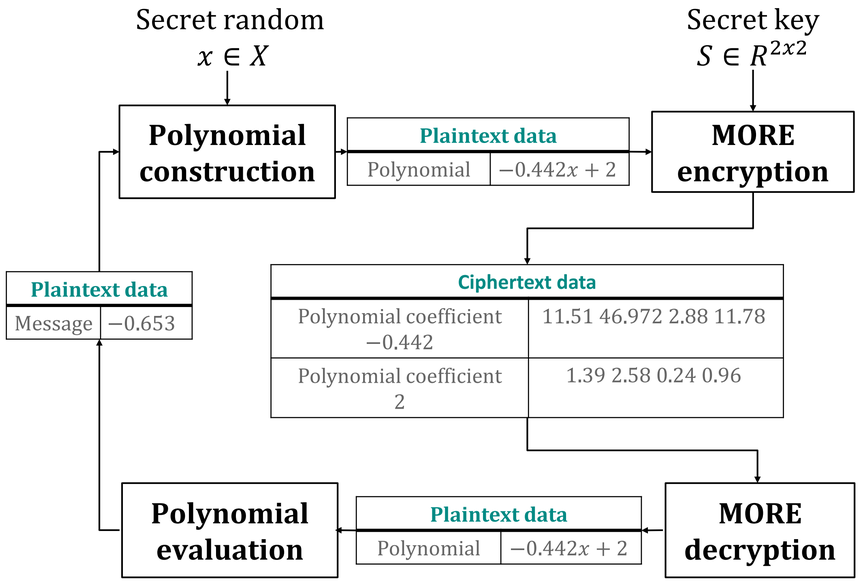


Figure 1. WBC parameter estimation network.

Hybrid MORE

Although MORE is an attractive choice due to its unbiased advantages in terms of performance and usability it implies a weaker security when used directly on rational numbers.

To increase scheme security an additional obfuscation layer based on polynomial evaluation maps is added.



Conclusion

Solution based on HE that promotes both security and availability by allowing DL algorithms to be used directly on encrypted data.

Strengthening the encryption scheme security, while maintaining the potential to be used in real-world applications, represents a work direction that should be further addressed.