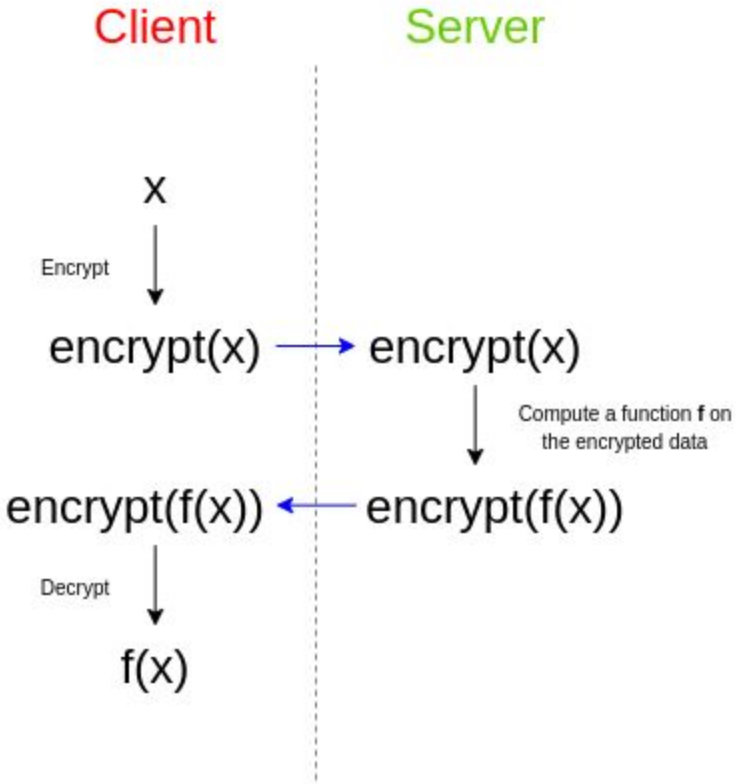
Homomorphic Encryption

Aakanksha Duggal
Senior Data Scientist
ET Data Science Team

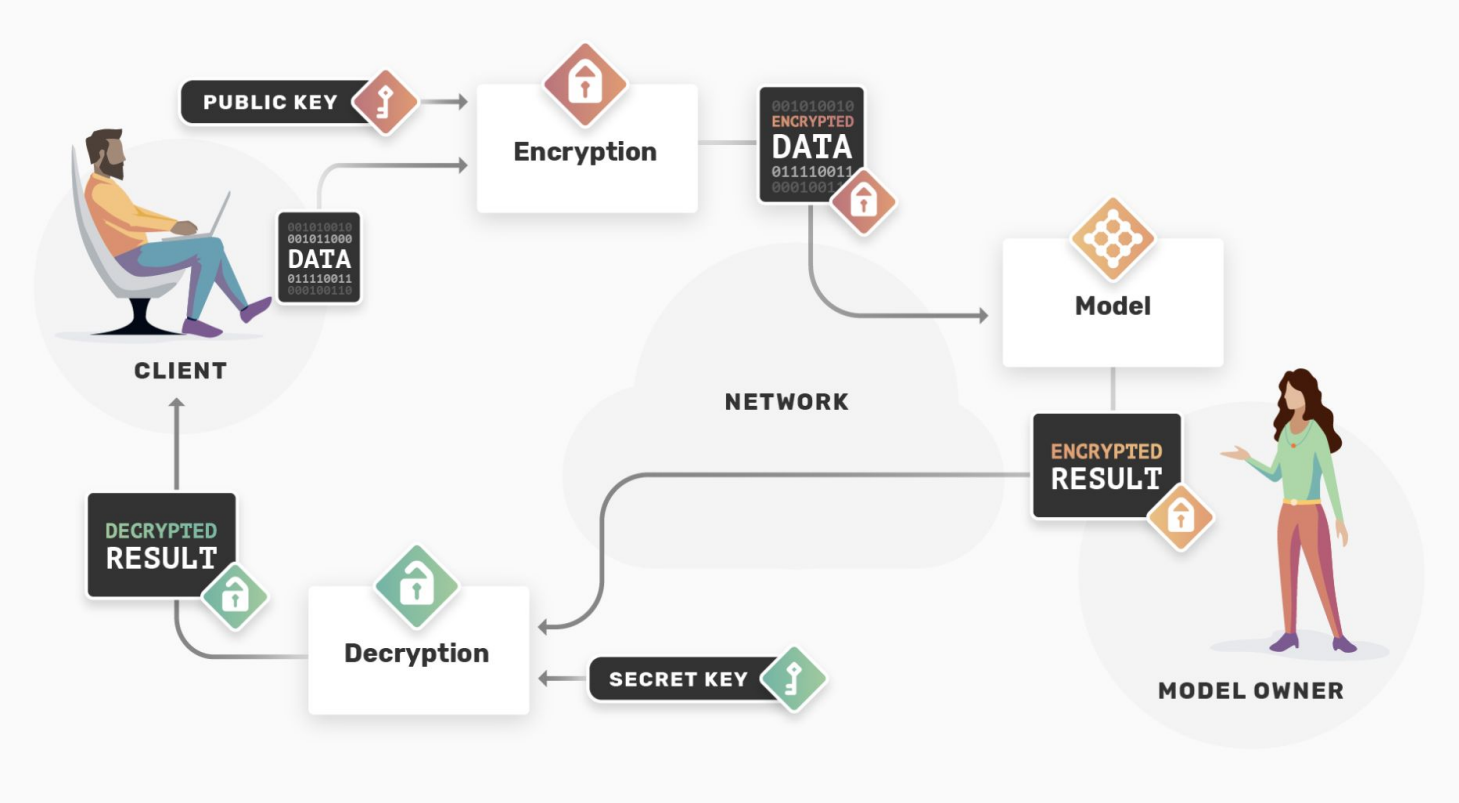
Red Hat

What is Homomorphic Encryption?



Red Hat

What is Homomorphic Encryption?



Red Hat

Applications of Homomorphic Encryption

Telco
Telecommunications

Software Companies

Transportation
Car

Government (general)
Government

Aerospace/defense
Fighter jet

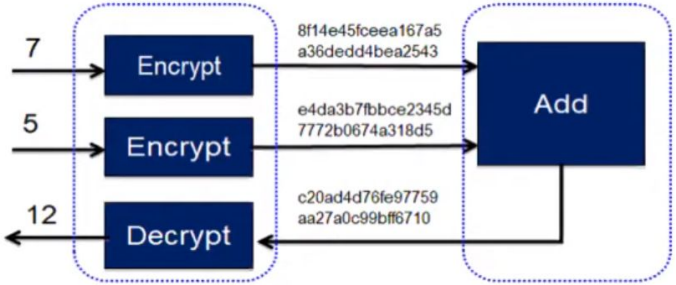
Healthcare
Heart monitor

Financial services
Money

Hybrid cloud infrastructure

Red Hat

Homomorphic Encryption



Advantages

- Perform inference on encrypted data
- No interaction between the data and the model owners
- Data Storage outsourcing

Disadvantages

- Computationally expensive
- Limited calculations and operations

Red Hat

Homomorphic Encryption

Partially HE (PHE)

Supports only one operation
“+ Or x”

Paillier Partially HE

Somewhat HE (SHE)

Supports only two operations
But limits to a certain operations.

BFV Scheme

Fully HE (FHE)

Can support any number of complex operations.

CKKS and BGV Scheme

Comparison Study

	+	-	x					
Pallier (PHE)	✔		✔					
BFV (SHE)	✔	✔	✔					
CKKS (FHE)	✔	✔	✔					

Comparison Study

	+	-	x	Python-paillier				
Pallier (PHE)	✔		✔	✔				
BFV (SHE)	✔	✔	✔	❌				
CKKS (FHE)	✔	✔	✔	❌				

Comparison Study

	+	-	x	Python-paillier	PySEAL/ SEAL-python			
Pallier (PHE)	✔		✔	✔	❌			
BFV (SHE)	✔	✔	✔	❌	✔			
CKKS (FHE)	✔	✔	✔	❌	✔			

Comparison Study

	+	-	x	Python-paillier	PySEAL	pyFHE		
Pallier (PHE)	✔		✔	✔	❌	❌		
BFV (SHE)	✔	✔	✔	❌	✔	✔		
CKKS (FHE)	✔	✔	✔	❌	✔	✔		

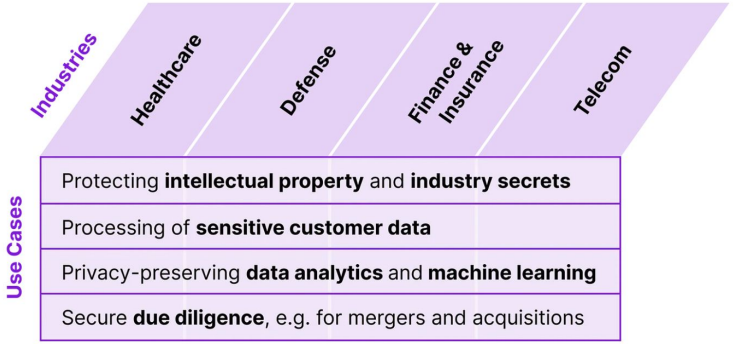
Comparison Study

	+	-	x	Python-paillier	PySEAL	pyFHE	PyFHEL	
Pallier (PHE)	✔		✔	✔	❌	❌	❌	
BFV (SHE)	✔	✔	✔	❌	✔	✔	✔	
CKKS (FHE)	✔	✔	✔	❌	✔	✔	✔	

Comparison Study

	+	-	x	Python-paillier	PySEAL	pyFHE	PyFHEL	TenSEAL
Pallier (PHE)	✔		✔	✔	❌	❌	❌	❌
BFV (SHE)	✔	✔	✔	❌	✔	✔	✔	✔
CKKS (FHE)	✔	✔	✔	❌	✔	✔	✔	✔

Homomorphic Encryption vs Confidential computing



Use cases and industries for which HE and CC are relevant

HE

- **No specialized hardware**
- Lack of hardware for compute intensive tasks
- Lack of attestation mechanism

CC

- **Works with hardware**
- Limited to a certain places to execute
- attestation mechanism ensures data and code integrity

Source : https://blog.edgeless.systems/the-differences-between-homomorphic-encryption-and-confidential-computing-and-when-to-use-what-bea3fb0ddfd

Red Hat

Thank you, questions?

- Github - https://github.com/redhat-et/homomorphic-learning/


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat