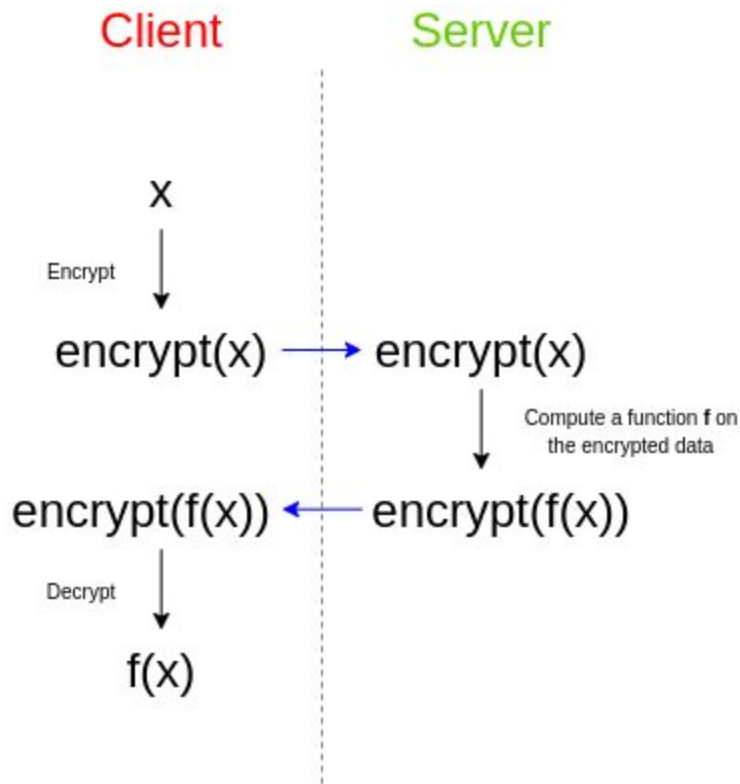# Homomorphic Encryption

Aakanksha Duggal
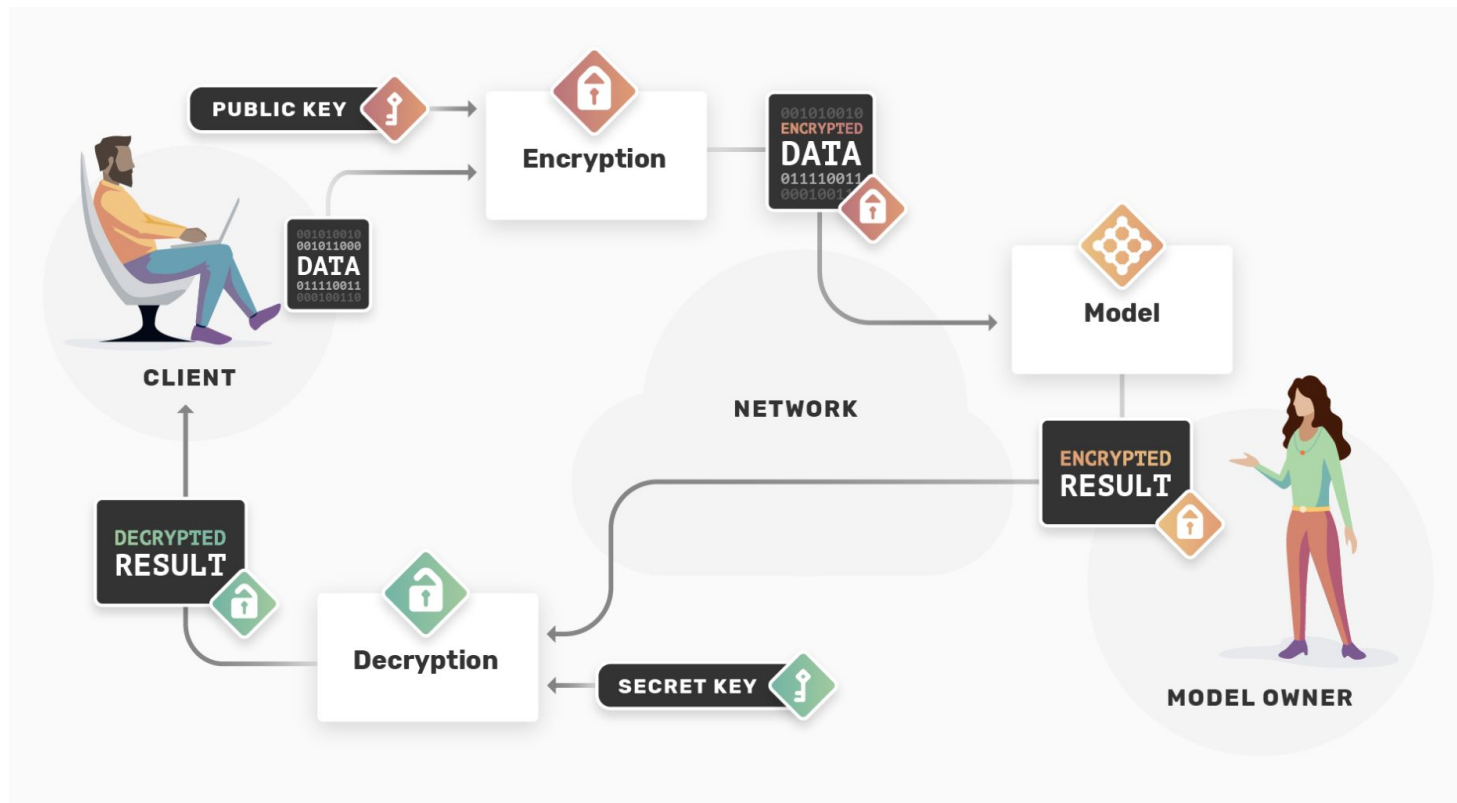
Senior Data Scientist

ET Data Science Team

Red Hat

What is Homomorphic Encryption?

What is Homomorphic Encryption?

Applications of Homomorphic Encryption

Telco
Telecommunications

Software Companies

Transportation
Car

Government (general)
Government

Healthcare
Heart monitor

Financial services
Money

Hybrid cloud infrastructure

Aerospace/defense
Fighter jet

Red Hat

Homomorphic Encryption
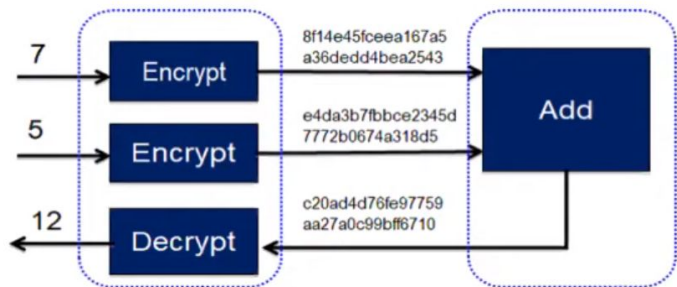
Advantages

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

Disadvantages

- Computationally expensive
- Limited calculations and operations

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

Red Hat

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)	✔	✔	✔	✘	✔	✔	✔	✔

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