IBM Fully Homomorphic Encryption

—

July 15, 2021

Meet the team

Pradeep Parameshwaran
IBM Systems
Security and Compliance Lead

Rohit Panjala
IBM Systems
Associate Product Manager

Agenda

1. FHE introduction
2. Use cases
3. Demo
4. Call to action

Enterprises today are facing tighter data privacy regulations and an advanced threat landscape

$360M

Total amount of GDPR fines issued from 692 cases since 2018

Every one of the 28 EU nations, plus the United Kingdom, has issued at least one GDPR fine

Source: Privacy Affairs
https://bit.ly/3cyEZsg

$2T

Estimated amount of money laundered globally in one year

Ineffective information sharing across institutions is a key reason why criminals get away

Source: The United Nations
https://bit.ly/3cAeOkZ

44%

of organizations had a breach caused by a 3rd party in the last year

74% said the breach occurred because too much privileged access had been granted

Source: Ponemon Institute
https://bit.ly/35u0F4S

$11M

The total average cost of an insider threat in 2020

60% of organizations had more than 20 incidents per year

Source: Ponemon Institute
https://ibm.co/2TTecjX

Delivering end to end security

EXISTING PROTECTIONS

Data at rest

Inactive data that is not currently being accessed or transferred

Data in transit

Travelling between public or private networks

INCREASING FOCUS

Data in use

Actively being accessed by an application or a user and stored in memory

Fully Homomorphic Encryption

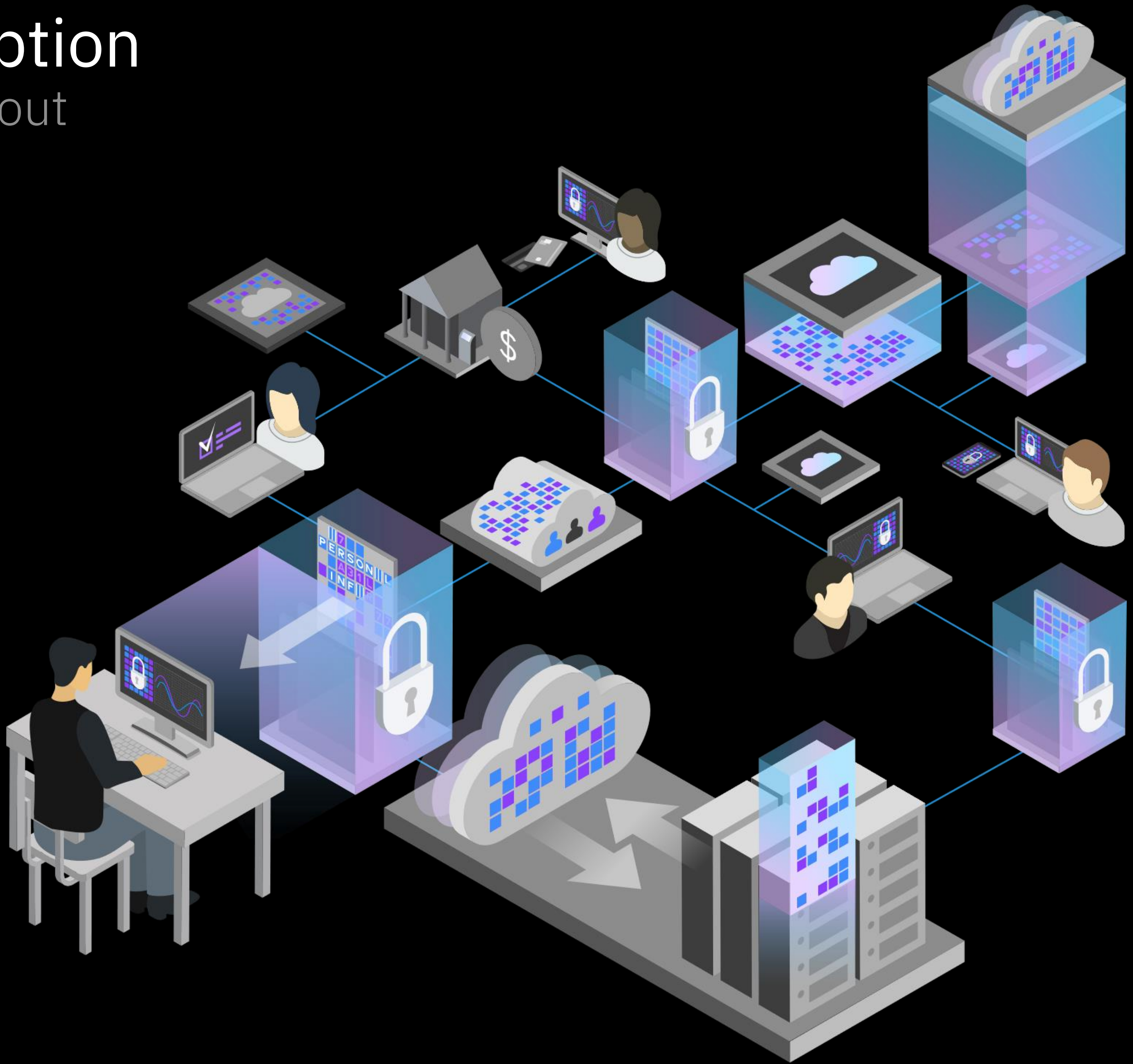
Compute upon encrypted data without decrypting it

Gain insights from sensitive data while preserving privacy

Enable AI, machine learning and data analytics to access encrypted data

Begin building quantum safe applications today with free toolkit

Confidently process and collaborate in public and private clouds and third-party environments

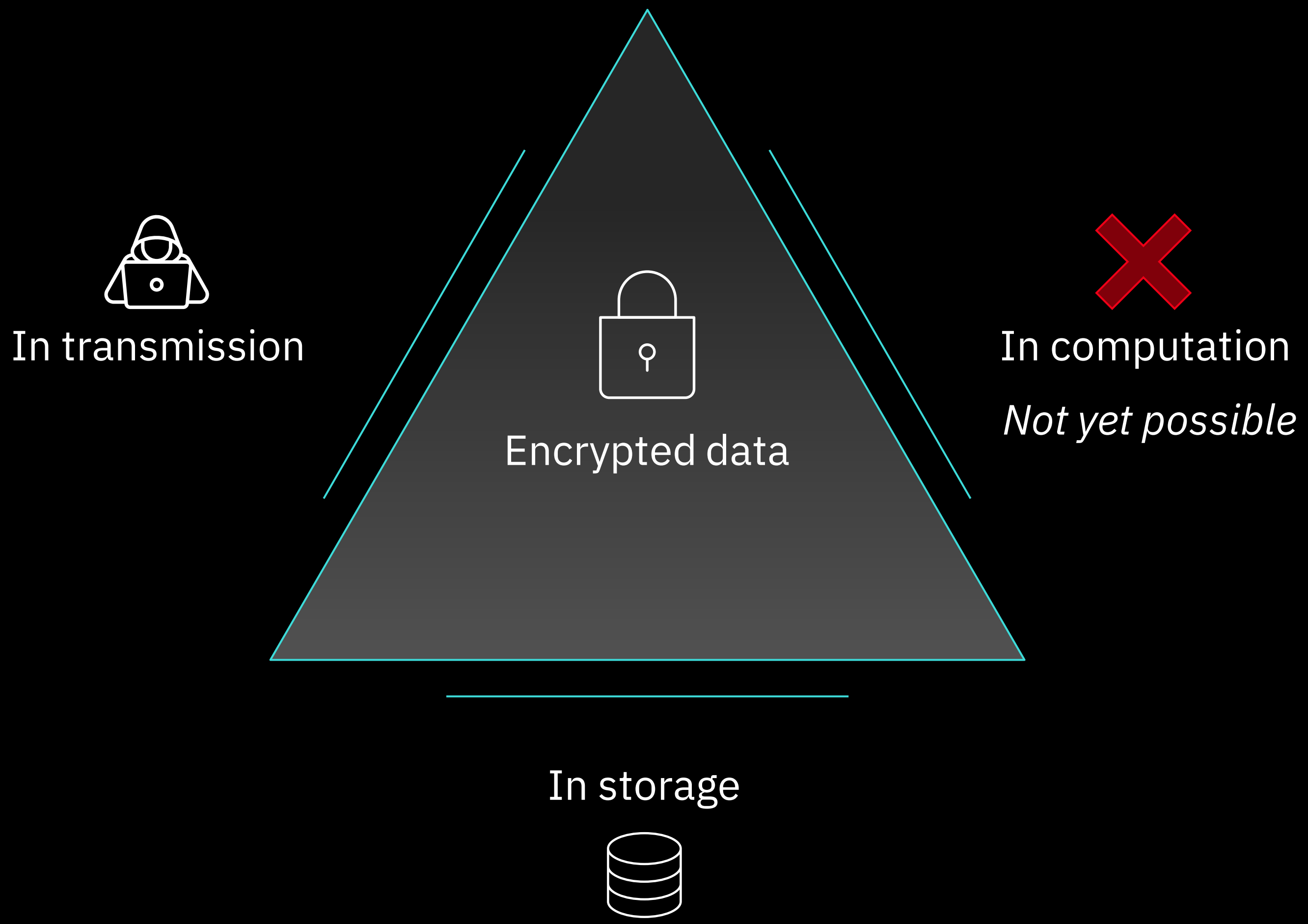


Fully Homomorphic Encryption

What is it and what can we do with it?

- ✓ ***Enables the processing of data without giving access to it.***
- ✓ ***Technically achieved by computing on encrypted data.***
- ✓ ***Resolves the paradox of "need to know" vs "need to share".***
- ✓ ***Uses Lattice Cryptography -> Quantum Resistant***

Security paradigm shift



Encrypted data

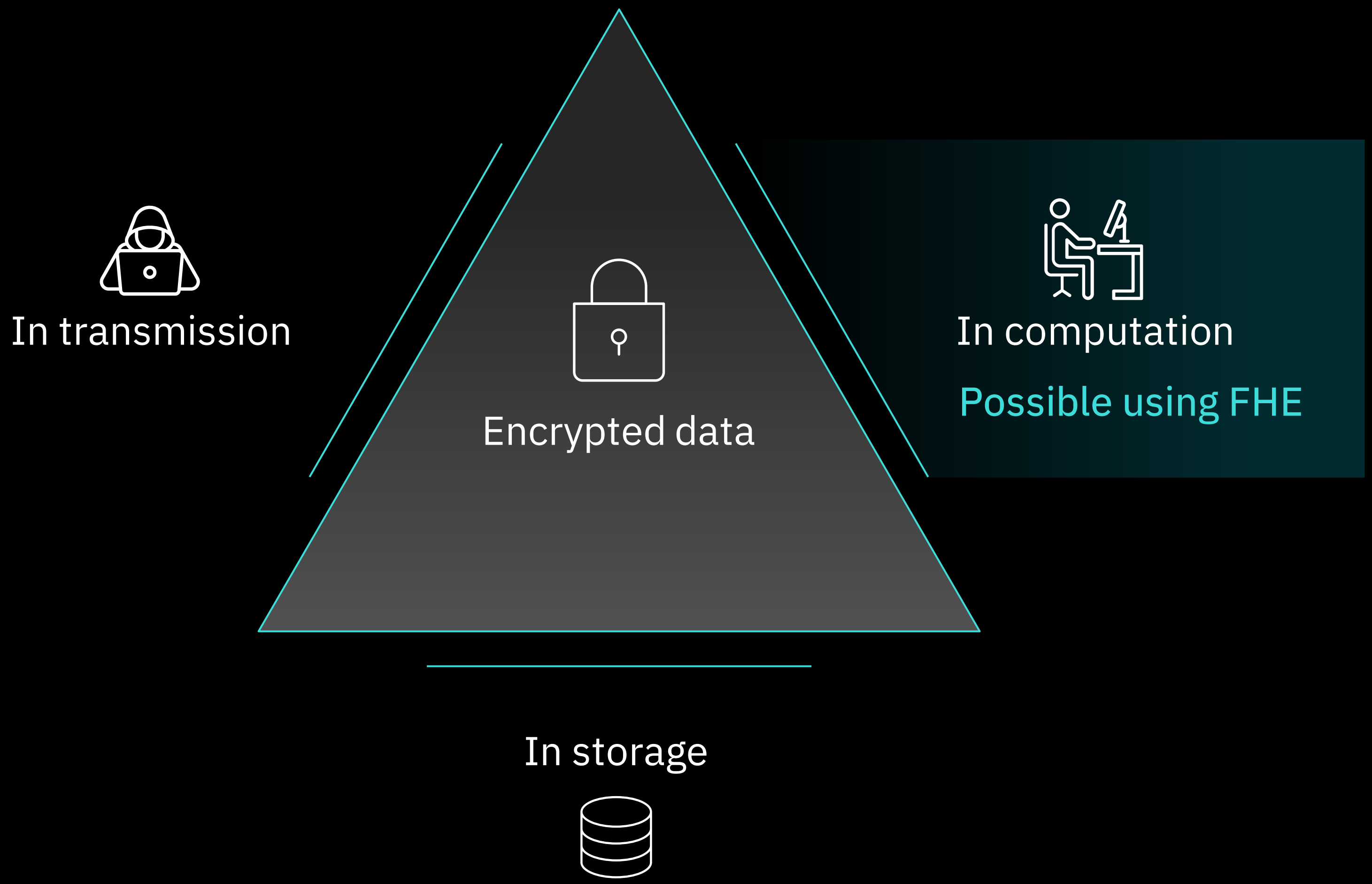
In transmission

In computation

Not yet possible

In storage

Security paradigm shift



Encrypted data

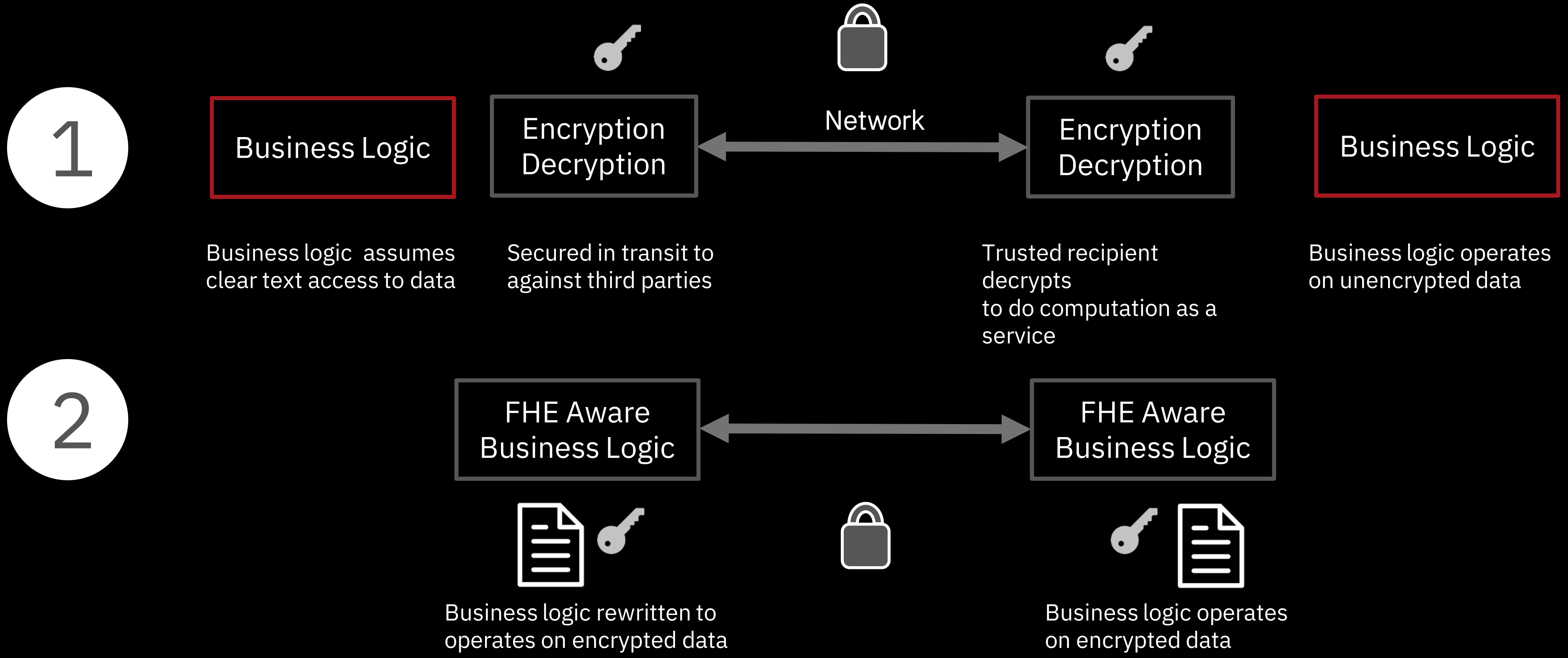
In transmission

In computation

Possible using FHE

In storage

Pervasive business logic security by design



1

Business Logic

Encryption Decryption

Network

Encryption Decryption

Business Logic

Business logic assumes clear text access to data

Secured in transit to against third parties

Trusted recipient decrypts
to do computation as a service

Business logic operates on unencrypted data

2

FHE Aware Business Logic

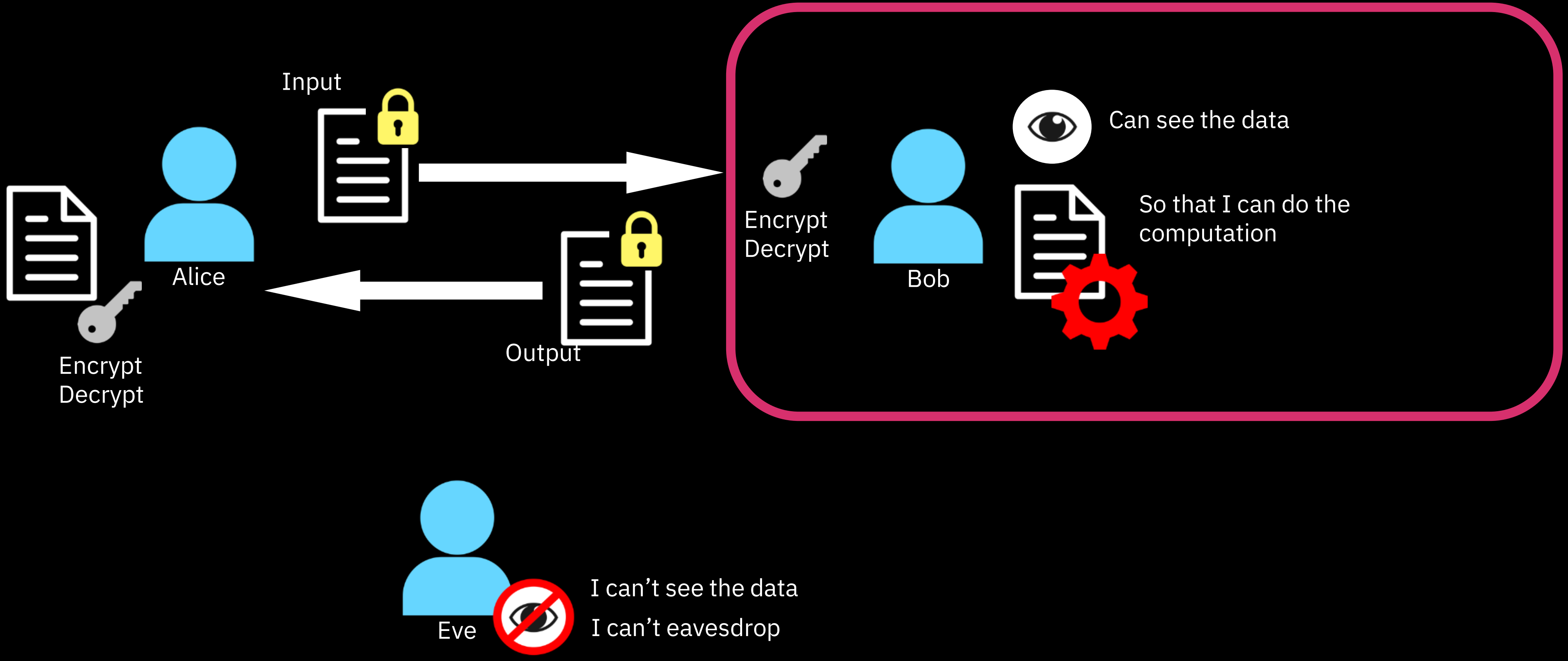
FHE Aware Business Logic

Business logic rewritten to operates on encrypted data

Business logic operates on encrypted data

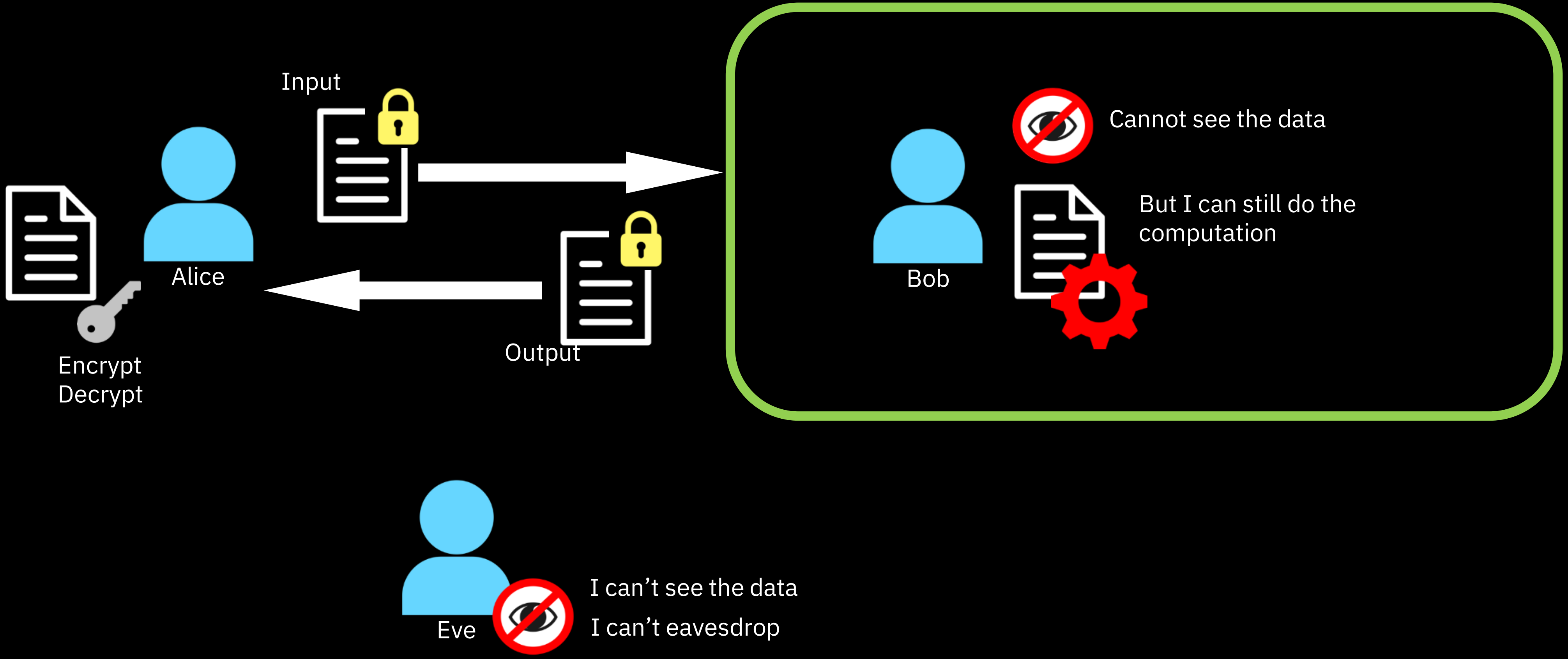
Computing on data today

Threat model: honest but curious



Computing on data securely and privately

Threat model: honest but curious



Input

Alice

Encrypt
Decrypt

Output

Bob

Cannot see the data

But I can still do the computation

Eve

I can’t see the data

I can’t eavesdrop

Unlock the value of your sensitive data

Use case archetypes

Privacy Preserving Search

FHE can enable customers to perform an encrypted query without revealing intent and search contents

Secure Cloud Computing

FHE can enable cloud adoption for customers who would never migrate their sensitive data due to security concerns

Statistics & Analytics on Encrypted Data

FHE can enable customers to perform operations on encrypted data without risking sensitive data exposure or disrupting workflows

Encrypted AI & Machine Learning

FHE can enable customers to train AI/ML models and run inferencing with sensitive data while preserving privacy and compliance

Unlock the value of your sensitive data

Use cases by industry

Use Case Archetypes

- 🟩 Privacy Preserving Search (search without revealing intent)
- 🟥 Cloud Computing (enabling increased cloud adoption)
- 🟦 Statistics (analytics without disclosure, e.g. set intersection)
- 🟪 AI/Machine Learning (insights without revealing data or models)

Financial Services	Healthcare	Defense	Energy	Telecommunications	Education
🟩 Fighting financial crime (AML, credit card theft)	🟩 Multi-center studies/research collective	🟩 Battlefield data encryption at the edge	🟩 Securing energy supply chain	🟩 Private mobile location services	🟦 Privacy preserving policy decisions
🟩 Customer Due Diligence (CDD, EDD, KYC)	🟩 Securing health care supply chain	🟩 Securing military supply chain	🟪 Secure energy optimization		
🟩 Cross-border data collaboration and analysis	🟩 Public health readiness	🟦 Private satellite collision prediction	🟪 Secure information aggregation for smart grids		
🟩 Monetize data and IP	🟩 Pharmaceutical pipeline development	🟪 Predictive maintenance for distributed fleets			
🟥 Migration to cloud and secure processing	🟦 Disease analysis				
🟦 Mergers and Acquisitions	🟦 Clinical trials patient selection				
🟦 Double blind trade matching	🟪 Real World Evidence studies				
🟪 Consumer credit modeling	🟪 Genetic risk prediction				
🟪 Protecting financial models from exfiltration	🟪 Genome-Wide Association Studies				

Fighting financial crime

Secure fraud detection

Problem

According to the Federal Trade Commission, consumers reported losing more than **$3.3 billion** related to fraud complaints in 2020.

Solution

With FHE, encrypted AI inferencing can be done on sensitive credit card data to detect fraudulent transactions while protecting data and insights.

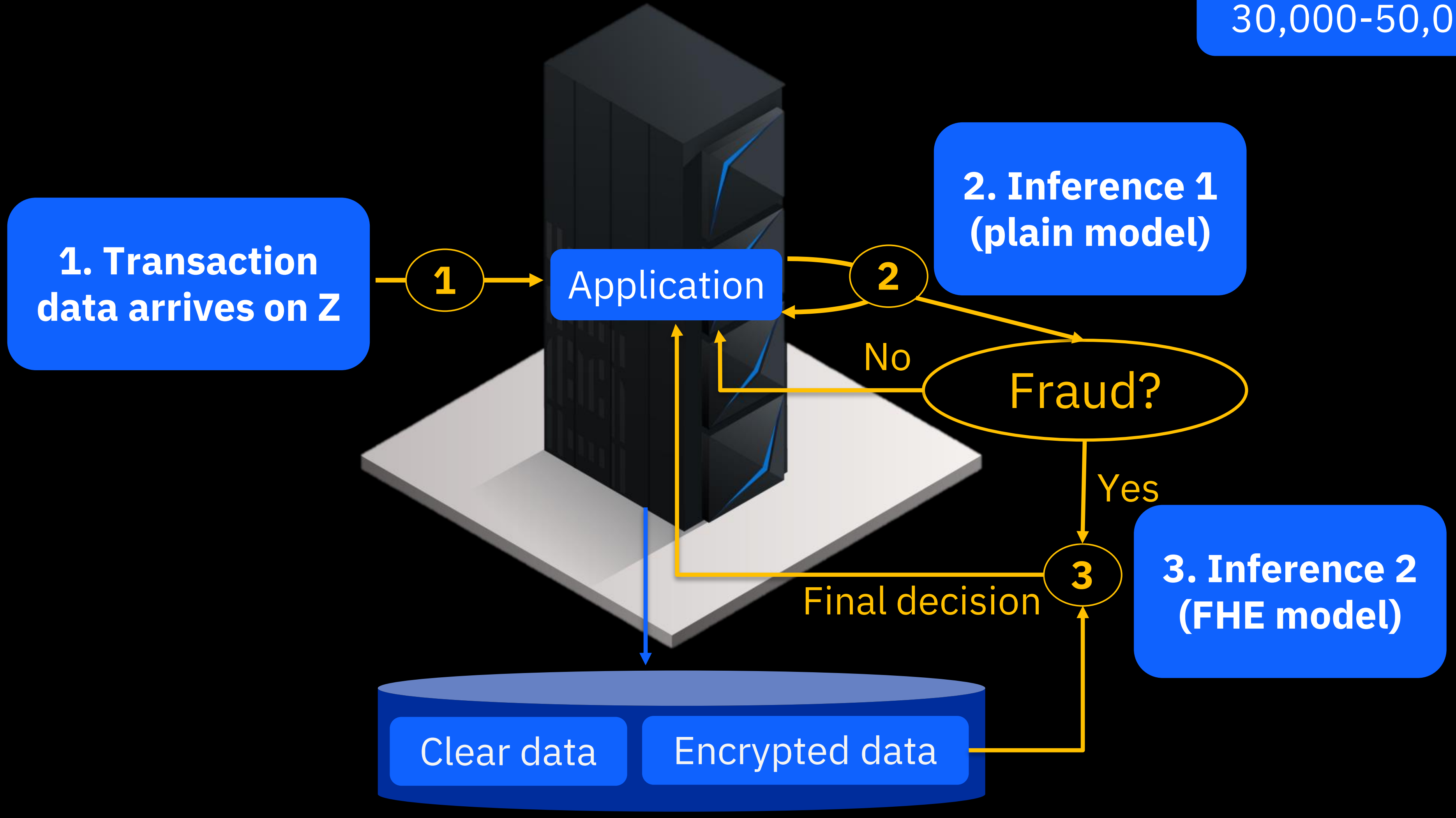
2021 Think Demo

Round trip inferencing time for a single transaction from Db2 on z/OS to FHE running on z/OS Container Extensions (zCX) is less than one second. Batch performance per transaction is in milliseconds.

Incorporate encrypted customer data to improve fraud detection

2021 Think demo

Overall SLA Requirements:
30,000-50,000 Transactions Per Second



1. Transaction data arrives on Z

1

Application

2

2. Inference 1 (plain model)

No

Fraud?

Yes

3

3. Inference 2 (FHE model)

Final decision

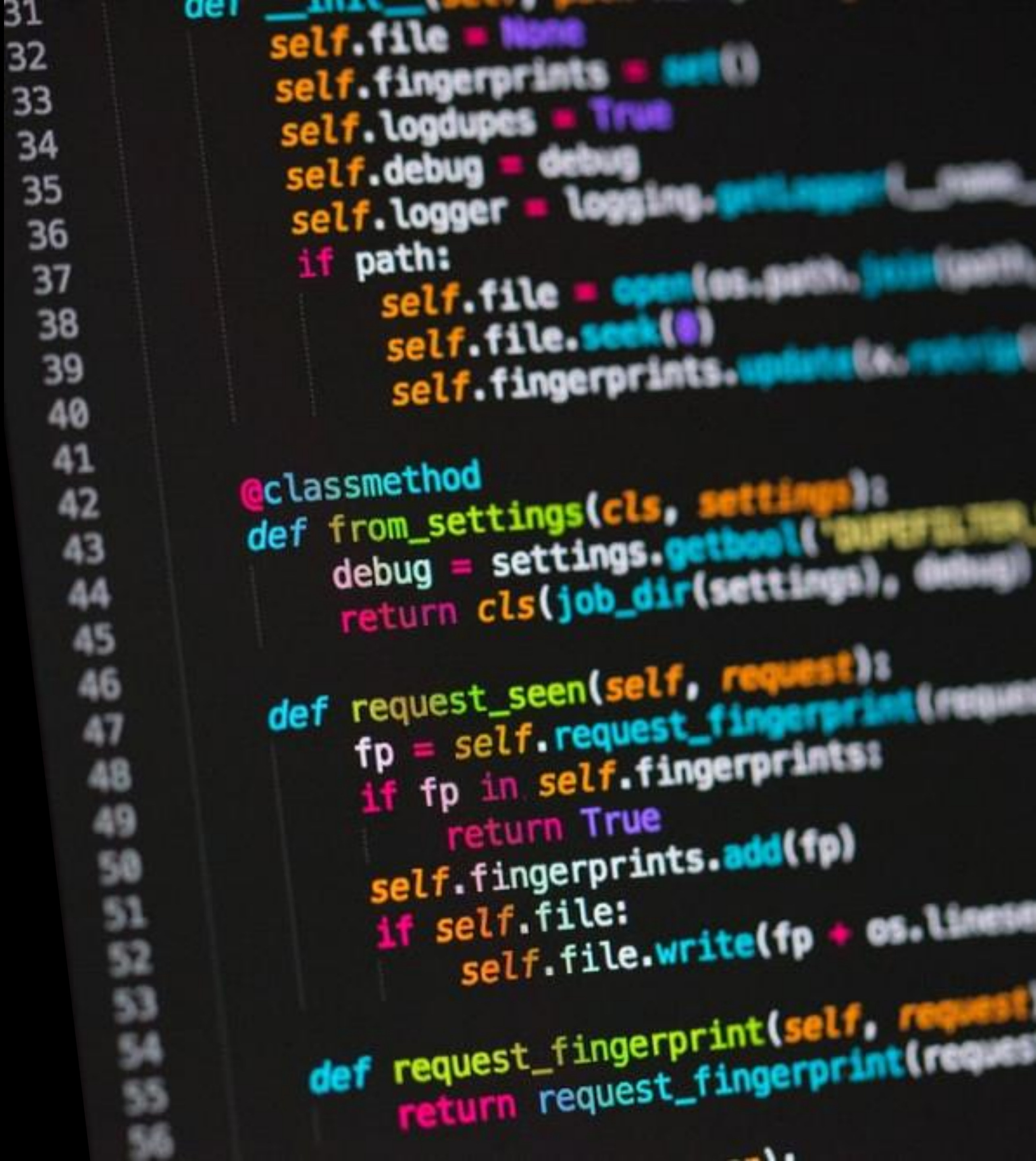
Clear data

Encrypted data

FHE demo

Secure fraud detection

- Encrypted AI inferencing using encrypted samples from a credit card transaction dataset
- Homomorphically encrypted neural network with 3 fully connected layers
- AI-SDK using CKKS scheme
- Python API
- Hosted on s390x



Why FHE on IBM Z & LinuxONE?

- The market is **strongly aligned** with the core client base with multiple use cases in financial services, healthcare, and insurance
- IBM’s control over the full stack (hardware, crypto libraries, software, services) provides a **significant competitive advantage**
- Systems level perspective needed for a production quality, highly secure and scalable FHE solution
- Large cache size, large memory, and proximity to highly sensitive data
- Strong experience with enterprise key management, which is critical for a production-ready FHE solution

FHE Toolkit

Free and open-source Linux based Docker container

What's inside?

- Ready-to-run example code
- Visual Studio code IDE
- IBM Homomorphic Encryption Library (HElib)

Two demos

- **Encrypted AI/ML** credit card fraud detection
- **Privacy preserving search** country/capital lookup

Runtimes

- Linux on Z
- z/OS Container Extensions
- Hyper Protect Virtual Servers
- Windows 10 Subsystem for Linux
- MacOS
- iOS

Distributions

- CentOS
- Fedora
- Ubuntu
- Alpine

IBM Research’s AI-SDK

Priced and proprietary

- Python and C++ APIs
- Import outputs from popular machine learning neural network models
- Support for a wide variety of machine learning models
- We choose the best model parameters for you
- Optimizer to select for throughput or latency with a single line of code
- Estimator for real latency and throughput
- Library and scheme agnostic

Fully Homomorphic Encryption Sponsor User Program

Partner

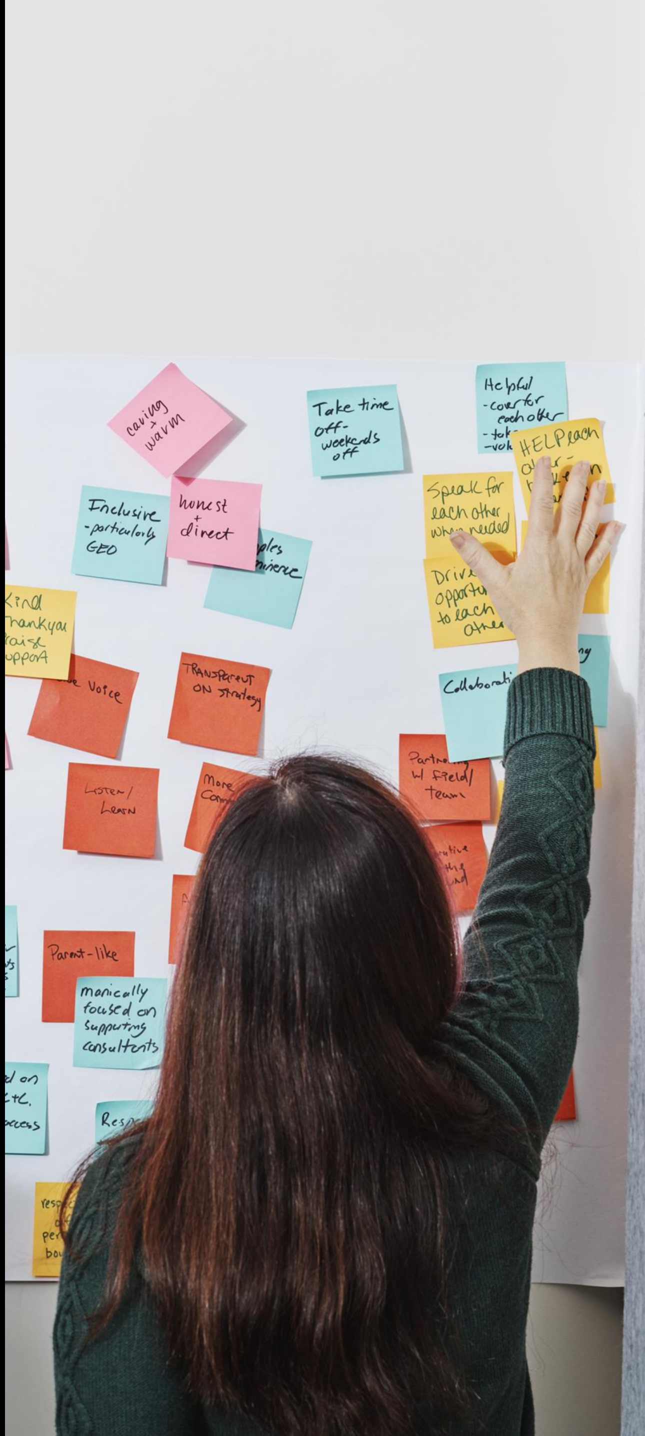
We are accepting FHE sponsor users at no cost and pursuing joint development opportunities

Who is invited?

We want to engage with application developers, data scientists, applied AI teams, crypto leads, and executives to refine the FHE user experience

Sign up

Email fhestart@us.ibm.com



Call to action

Read

Content Solutions Page
Link

IBM Developer Blog
Link

Linux Announce Blog
Link

Participate

Technical Deep Dive
Email fhestart@us.ibm.com

Sponsor User Program
Email fhestart@us.ibm.com

FHE Toolkit for Linux
Link

Media

Terminal Talk Podcast
Link

IBM YouTube
Link

Open Mainframe Summit
Link

Thank You!
Questions?

Pradeep Parameshwaran
Security and Compliance Lead
pradeep@de.ibm.com
—
Rohit Panjala
Associate Product Manager
rohit.panjala@ibm.com