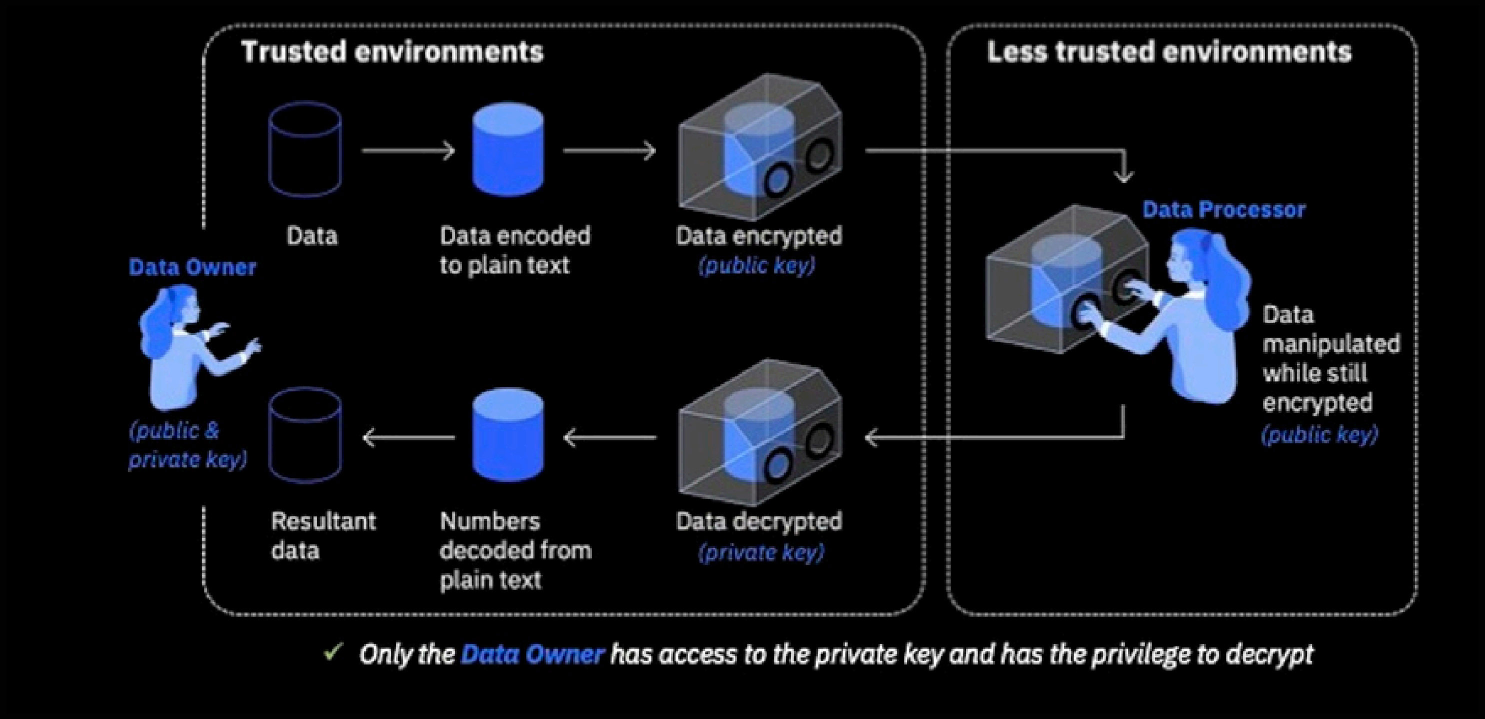
SEKURENET

Real-World Applications of Fully Homomorphic Encryption (FHE)

SEKURENET

What is Fully Homomorphic Encryption?


Trusted environments
Less trusted environments
Data
Data encoded to plain text
Data encrypted (public key)
Data Owner
(public & private key)
Data Processor
Data manipulated while still encrypted (public key)
Resultant data
Numbers decoded from plain text
Data decrypted (private key)
✓ Only the Data Owner has access to the private key and has the privilege to decrypt

FULLY HOMOMORPHIC ENCRYPTION (FHE) IS A FORM OF ENCRYPTION THAT ALLOWS COMPUTATIONS TO BE PERFORMED DIRECTLY ON ENCRYPTED DATA WITHOUT NEEDING TO DECRYPT IT. THE RESULT OF THESE COMPUTATIONS REMAINS ENCRYPTED AND CAN ONLY BE DECRYPTED BY THE AUTHORIZED PARTY USING THE CORRECT DECRYPTION KEY.

Applications

✅ 1. Secure Data Processing in the Cloud

- **Problem:** Organizations store sensitive data in the cloud but fear data breaches and unauthorized access.

- **Solution:** With FHE, encrypted data can be processed without decryption, ensuring complete privacy.

- **Example:** Financial institutions can perform risk analysis on encrypted customer data without exposing it to the cloud provider.

✅ 2. Regulatory Compliance and Data Sovereignty

- **Problem:** Organizations struggle to meet compliance regulations like GDPR and HIPAA when using third-party services.
- **Solution:** FHE ensures data remains encrypted during processing, minimizing the risk of non-compliance.
- **Example:** Financial services companies can outsource data analysis to cloud providers while maintaining regulatory compliance.

✅3. E-Voting Systems

- **Problem:** Digital voting systems are susceptible to fraud and privacy breaches.

- **Solution:** FHE ensures votes remain encrypted throughout the voting and counting processes.

- **Example:** Voters can cast encrypted ballots, and the results can be computed without revealing individual votes.

✅ 4. Privacy-Preserving Machine Learning (PPML)

Problem: Companies may need to analyze sensitive datasets for AI model training without compromising data privacy.

Solution: FHE enables secure computation on encrypted data for model inference and training.

Example: Healthcare providers can share encrypted patient data with AI models for disease prediction without revealing sensitive information.