ENCRYPT Privacy Preserving Technologies,

Use Cases and Opportunities

encrypt

Core Privacy-Preserving Technologies in ENCRYPT

- Fully Homomorphic Encryption (FHE)
- Trusted Execution Environments (TEEs)
- Differential Privacy (DP)
- Hybrid Protection Services

encrypt

The Challenge: Protecting Data in Use

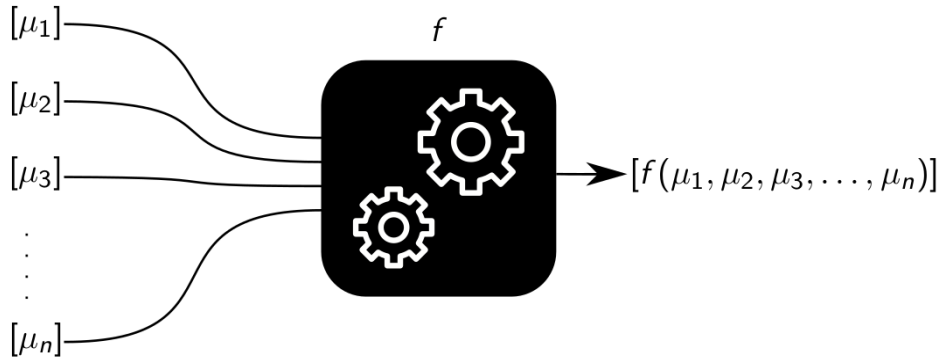
- Traditional security methods protect data at rest and in transit
- Data in use remains vulnerable during computation
- Risks include exposure of plaintext data to malicious actors

- Most popular approaches to shield computations
  - ✓Homomorphic Encryption (HE)
  - ✓Trusted Execution Environment (TEE)

- Both of these are part of ENCRYPT Technologies

What is Homomorphic Encryption (HE)?

- HE allows computations on encrypted data without decryption
  - ✓Ensures data confidentiality throughout processing.
  - ✓Enables secure computation in untrusted environments.
  - ✓Server has no information on the clear data, not even the result of its own computations.



encrypt

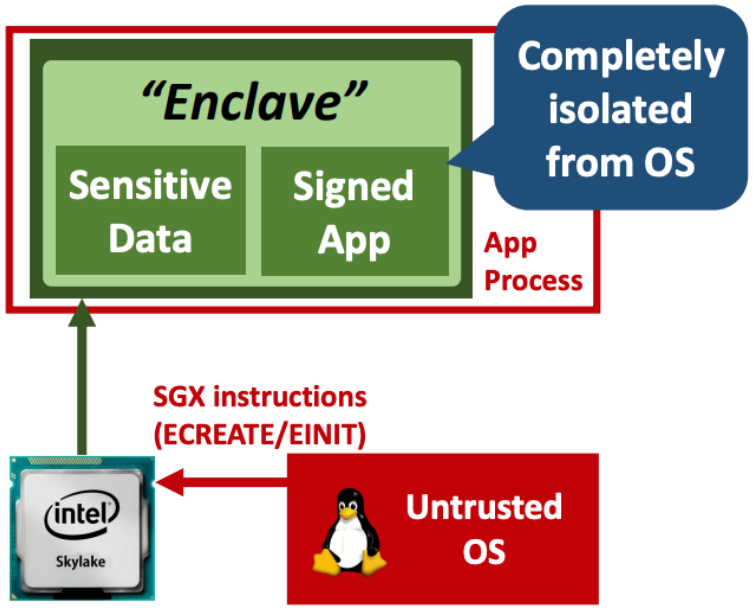
HE: Strengths and Weaknesses

- **Strengths**
  - ✓Highly Secure
  - ✓Ideal for privacy-sensitive applications
  - ✓Enables secure cloud computation

- **Weaknesses**
  - ✓High computational overhead
  - ✓Poor performance for complex, real-time tasks.
  - ✓Need to interact with the owner of the secret-key for each decryption
  - ✓Cipher Text Expansion (CTE)
  - ✓Unverifiable Conditionals

What is Trusted Execution Environment (TEE)?

- A hardware-based secure area within a processor
- Isolates sensitive computations and protects plaintext data
- Ensures trust in the execution of critical tasks



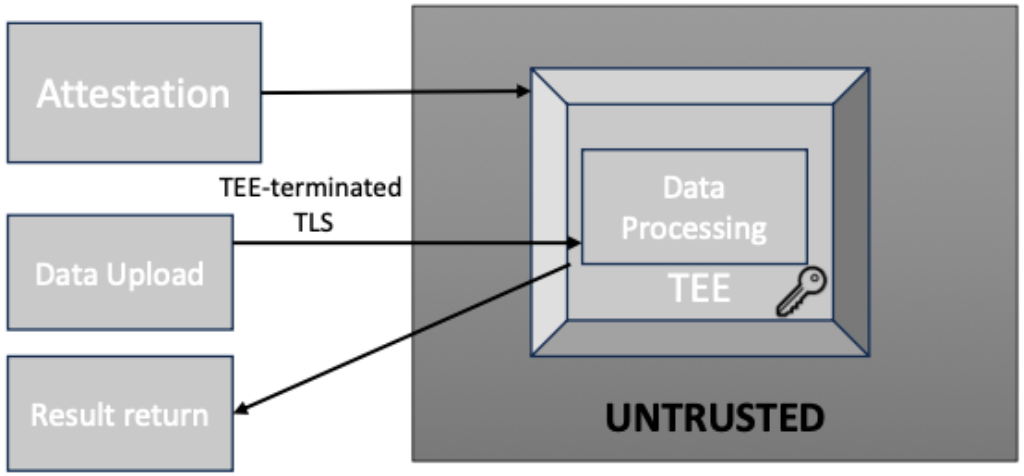
TEE: Strengths and Weaknesses

- **Strengths**
  - ✓High performance for plaintext processing
  - ✓Hardware-enforced isolation
  - ✓Practical for real-time applications

- **Weaknesses**
  - ✓Relies on trust in the hardware manufacturer
  - ✓Vulnerable to side-channel attacks
  - ✓Limited memory size

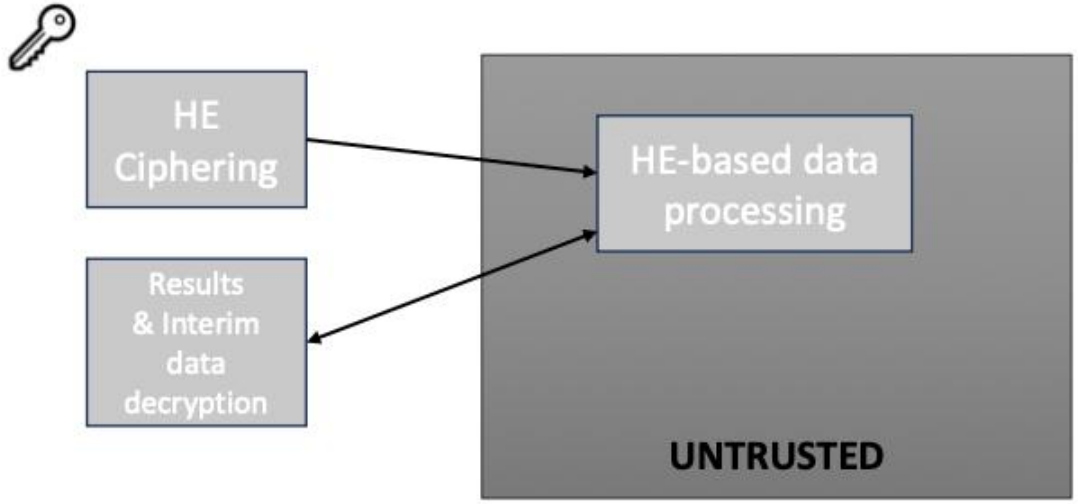
HE and TEE model summary

TEE



Clients attest the TEE and send confidential data. The computation occurs in the TEE.

HE



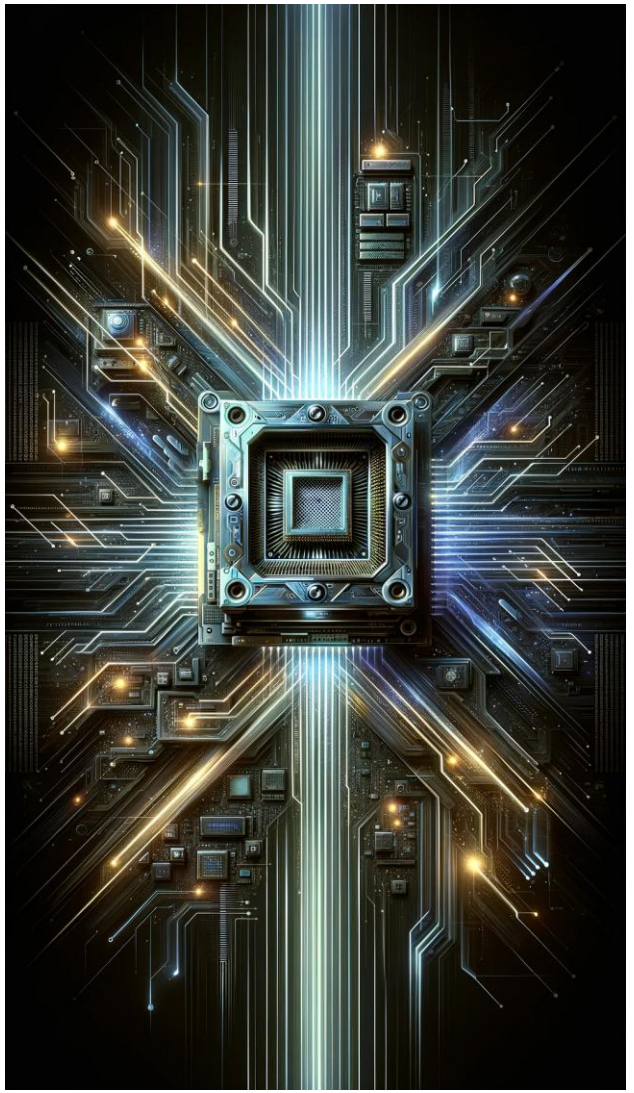
Clients generate HE keys and send HE confidential data. The computation occurs in the untrusted world on HE data.

Hybrid Solution: SOTERIA overview

- Mitigates the limitations of each technology
  - ✓Enhanced security: Confidentiality via HE, minimal TEE exposure
- Only encryption/decryption occurs within the TEE
  - ✓use counter-measures to side-channel attacks
- Strengths
  - ✓Highly Secure
  - ✓No side-channel Attacks
  - ✓Can verify conditionals and perform the HE ciphering/deciphering in trusted area
  - ✓best-suited HE scheme

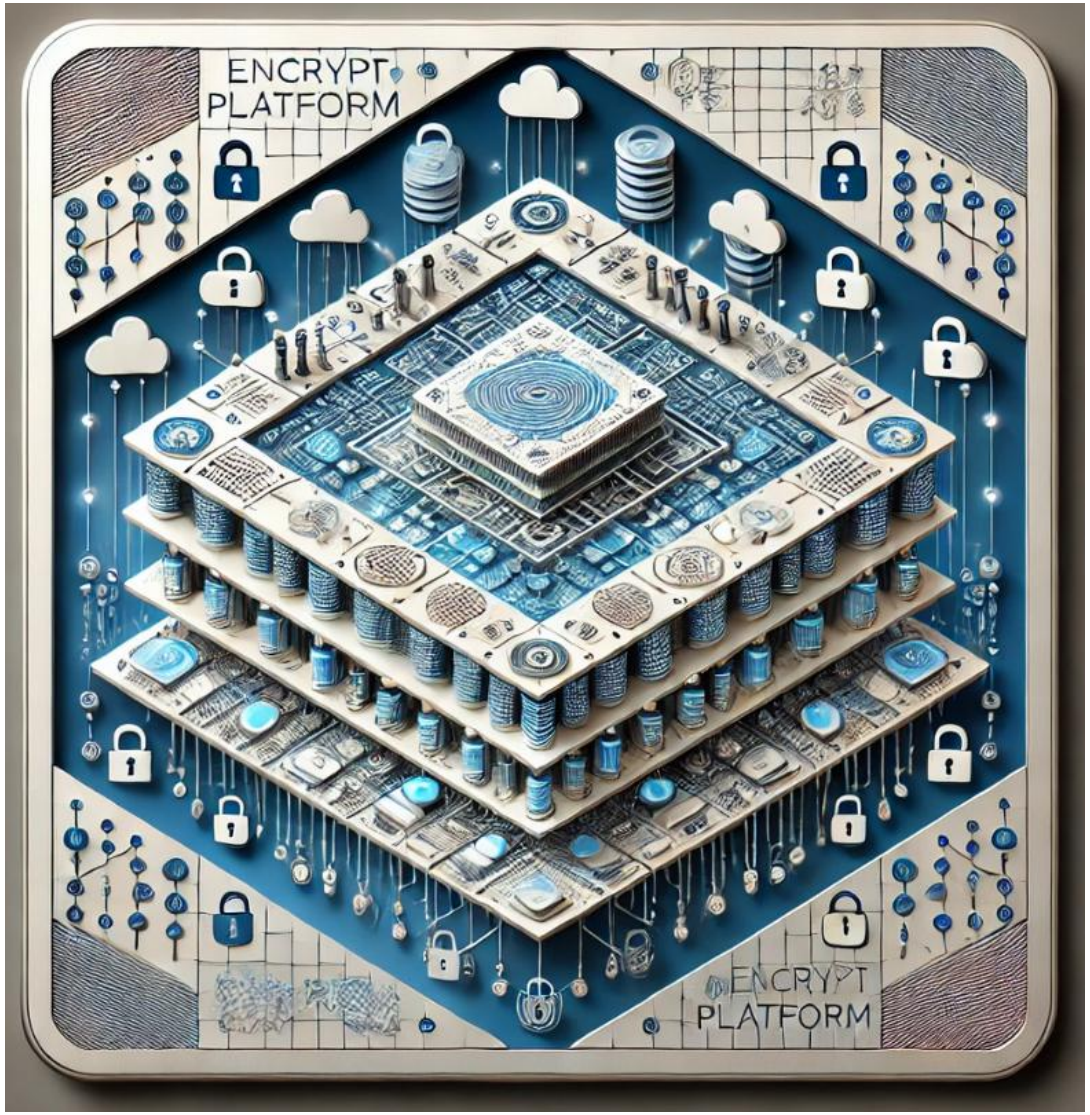
Boosting Performance with Hardware Acceleration

- Enhancing Computational Efficiency
  - ✓Offloads intensive tasks to specialized hardware (eg, GPUs)
  - ✓Reduces processing time for complex cryptographic operations
- Optimizing PPTs
  - ✓Improves the performance of Privacy-Preserving Technologies
  - ✓Makes advanced encryption methods more practical use
- Energy Efficiency
  - ✓Decreases energy consumption during data processing
  - ✓Supports sustainable and scalable privacy solutions
- Scalability
  - ✓Enables processing of larger datasets without compromising speed
  - ✓Critical for handling data in sectors like healthcare and finance
- Real-World Impact
  - ✓Enhances the overall usability and adoption of the ENCRYPT
  - ✓Facilitates faster and more secure data analysis



The ENCRYPT Platform Architecture

- Integrated Platform
  - ✓ Combines advanced PPTs for comprehensive data protection
  - ✓ Ensures scalability and efficiency in data processing
- AI-Powered Recommendation System
  - ✓ Suggests the best PPTs based on data type and context
  - ✓ Simplifies the selection process for users of varying expertise levels
- GDPR Compliance
  - ✓ Designed to meet and exceed GDPR requirements
  - ✓ Provides legal and ethical data processing solutions
- Sector-Specific Applications
  - ✓ Tailored for use cases in healthcare, finance, and cybersecurity
  - ✓ Demonstrates versatility across different industries



encrypt

Key Functionalities of the ENCRYPT Platform

- Pre-processing Tool
  - ✓Prepares data for secure processing
  - ✓Identifies and handles Personally Identifiable Information (PII)
- AI-Powered Recommendation System
  - ✓Suggests optimal Privacy-Preserving Technologies
  - ✓Adapts recommendations based on data characteristics and requirements
- Knowledge Graphs
  - ✓Enhances data interoperability and understanding
  - ✓Creates a semantically rich, interconnected data web
- Risk Assessment Tool
  - ✓Evaluates privacy and security risks
  - ✓Provides actionable insights for risk mitigation
- User-Centric Design
  - ✓Interfaces designed for ease of use across expertise levels
  - ✓Ensures accessibility and effectiveness for diverse users

Securing Financial Data in Fintech

- Focus on Financial Sector
  - ✓Application of ENCRYPT technologies in finance
  - ✓Protects sensitive financial data and customer information
- Key Technologies Used
  - ✓FHE for secure data processing
  - ✓DP to ensure privacy while analyzing financial data
  - ✓Trusted Execution Environments (TEEs) for secure computation
- Benefits
  - ✓Enables secure data sharing and processing across finance
  - ✓Ensures compliance with GDPR and other regulations
  - ✓Enhances customer trust by safeguarding their data
- Operational Efficiency
  - ✓Facilitates secure and efficient data analysis
  - ✓Supports innovation in financial services while maintaining privacy

encrypt

Protecting Patient Data in Healthcare

- Focus on Healthcare Sector
  - ✓Application of ENCRYPT technologies to secure patient data
  - ✓Ensures confidentiality during research & clinical operations
- Key Technologies Used
  - ✓FHE for secure data analysis
  - ✓TEEs to protect sensitive health data
  - ✓DP to anonymize patient data while maintaining utility
- Benefits
  - ✓Facilitates secure sharing of health data across institutions
  - ✓Supports compliance with GDPR and healthcare regulations
  - ✓Enhances patient trust by ensuring data privacy
- Advancing Healthcare Research
  - ✓Enables the development of personalized medicine
  - ✓Promotes collaboration in healthcare research

encrypt

Strengthening Cybersecurity with ENCRYPT

- Focus on Cybersecurity Sector
  - ✓Application of ENCRYPT technologies to enhance cybersecurity
  - ✓Protects sensitive information during threat analysis and data sharing
- Key Technologies Used
  - ✓Trusted Execution Environments (TEEs) for secure threat data processing
  - ✓Fully Homomorphic Encryption (FHE) to protect data during analysis
- Benefits:
  - ✓Enables secure sharing of threat intelligence across organizations
  - ✓Protects proprietary and sensitive data from exposure
  - ✓Enhances collective defense mechanisms through secure collaboration
- Mitigating Risks
  - ✓Balances the need for open threat data sharing with privacy protection
  - ✓Strengthens cybersecurity posture without compromising sensitive information

Opportunities for you!

- ENCRYPT experts are available to advise you on your data and analytic needs
- We can recommend to you the best ways with which you can prepare your data and which privacy preserving technology will be best for you to use
  - ✓There is no need for you to send us any private data, synthetic data, or even data attributes and their description would be a start
- We can then consider further collaboration between us.

Thank you!

Stay in touch

https://encrypt-project.eu/

encrypt-project

@encrypt_project

encrypt