Democratizing access to Privacy-Preserving Technologies

Enhancing Performance and Security

The combination of HE and TEE

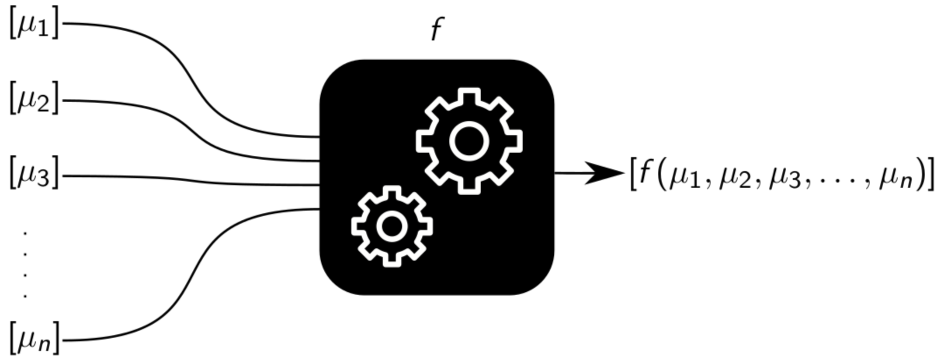
The Challenge: Protecting Data in Use

- 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)

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.



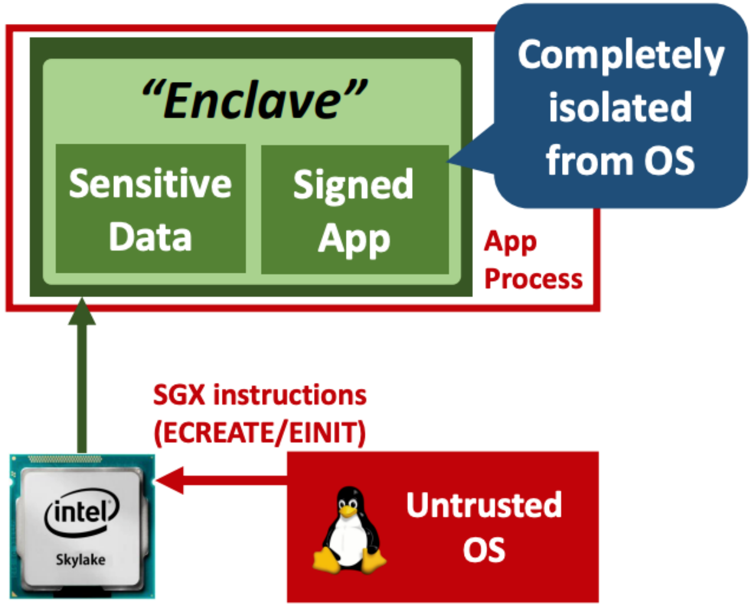
HE: Strengths and Weaknesses

- **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



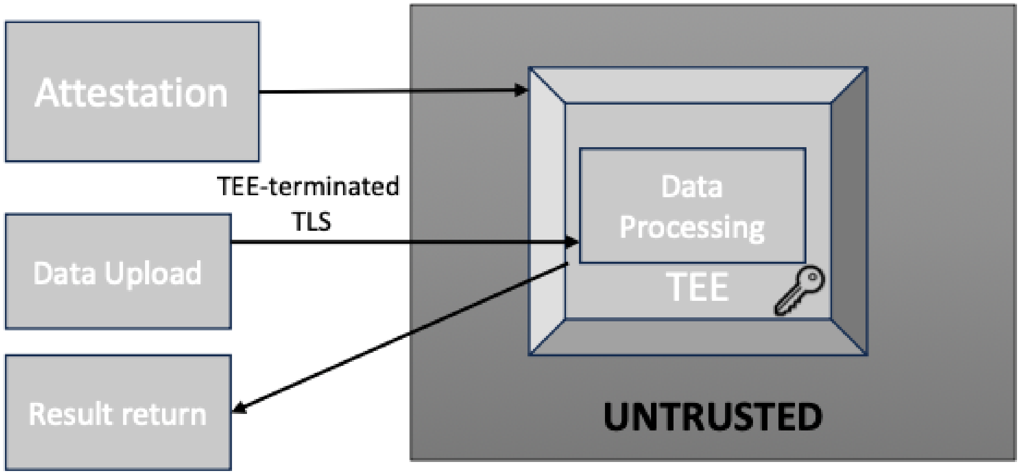
TEE: Strengths and Weaknesses

- **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

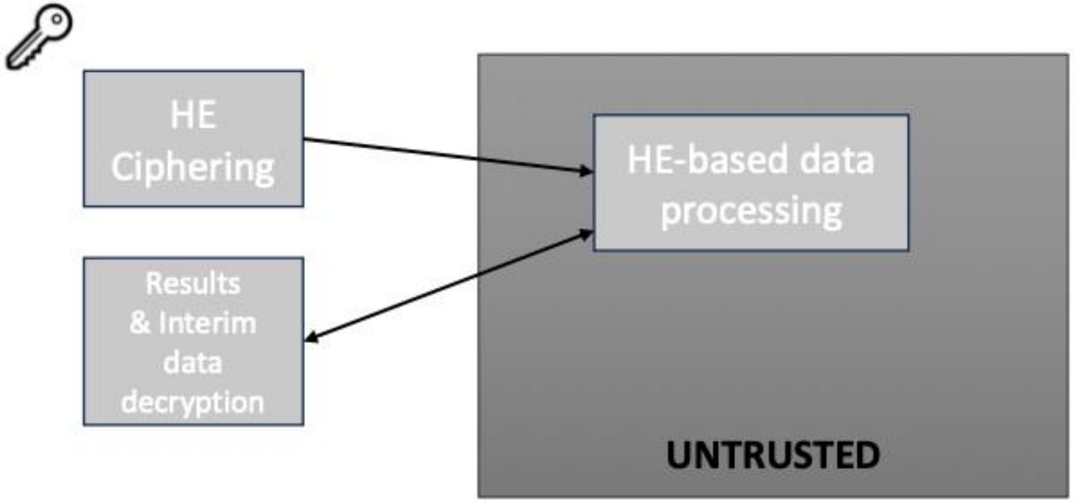
HE and TEE model summary

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

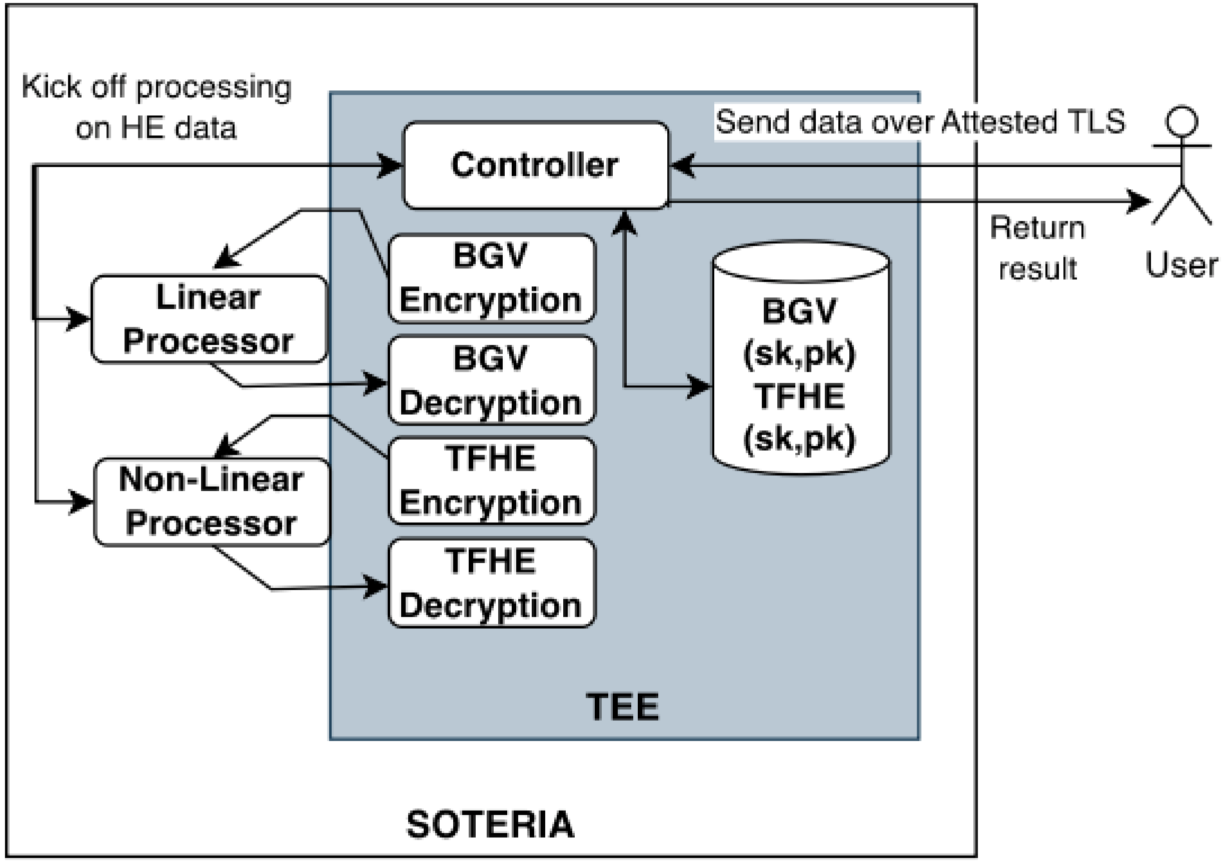
- Mitigate the limitations of each technology
  - ✓ Enhanced security: Confidentiality via HE, minimal TEE exposure

- 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

SOTERIA overall design

- Data is encrypted using an appropriate HE scheme
- TEE manages cryptoscheme switching for linear and non-linear operations
- Hybrid processing balances efficiency and security
- Obfuscation techniques, like flooding, enhance resilience



SOTERIA Design - Overall Design

- Initialization Phase:
  - ✓Data sent to TEE Controller for secure processing
  - ✓Secure TLS channel with remote attestation
  - ✓HE keys generated and sealed inside TEE
  - ✓Data encrypted with appropriate HE scheme (BGV/BFV or TFHE)

- Processing Phase
  - ✓Linear Processor: BGV/BFV for SIMD operations
  - ✓Non-Linear Processor: TFHE for fast evaluation
  - ✓Controller handles results and switches crypto-schemes for the next phase

SOTERIA Design - Security Protections

- Against Side-Channel Attacks
  - ✓TEE performs only cryptographic tasks
  - ✓Minimal plaintext exposure time
  - ✓Standardized protections for encryption/decryption

- Against TEE Compromise
  - ✓Flooding: Randomized and dummy ciphertexts obscure data
  - ✓Protects against TEE backdoors.

SOTERIA Design - Optimized Computation

- Optimizing HE Computation
  - ✓Combines linear and non-linear operations efficiently
  - ✓Selects best-suited HE scheme for each phase
  - ✓Supports large AI algorithm depth without parameter size increase

Thank you!

Stay in touch

https://encrypt-project.eu/

encrypt-project

@encrypt_project