

Framework of Secret Differential Privacy on Private Data

Problem Statement

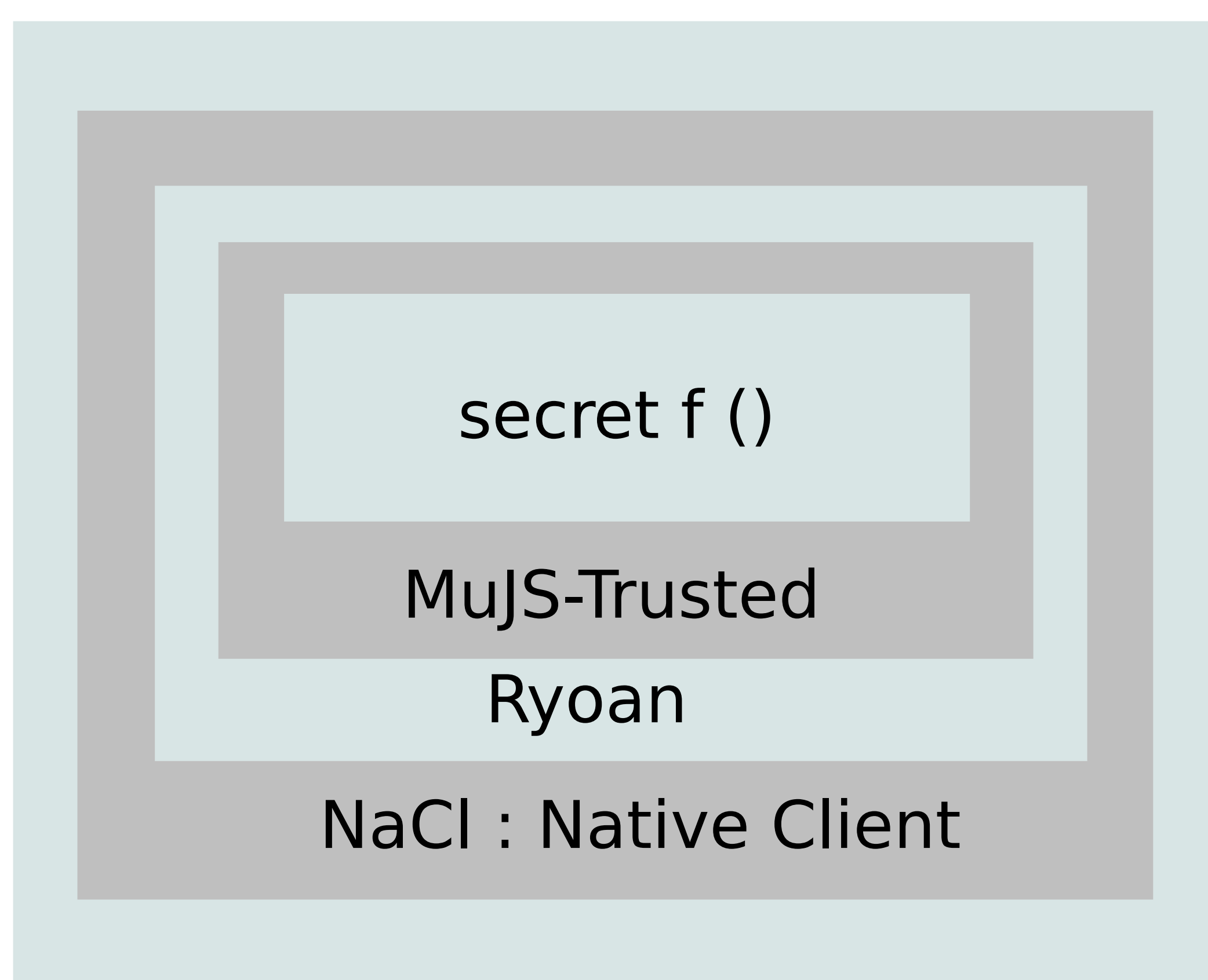
Valuable data processing applications are deployed in cloud servers. This **leaks the algorithm** to the host, and the algorithm may leak information about the processed data.

Challenges

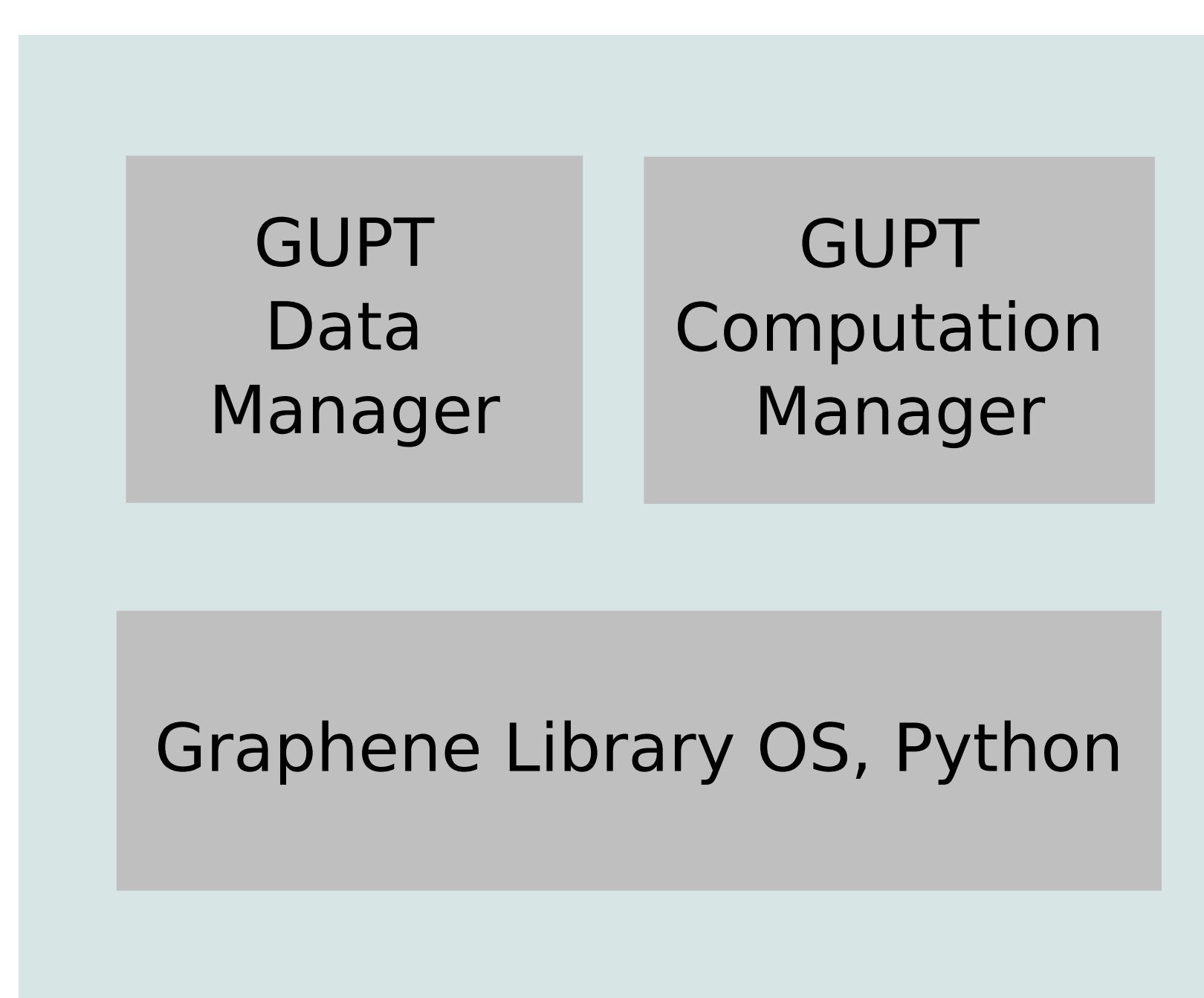
- **Sandboxing** of $f()$: Isolation of Differential Privacy framework from $f()$ function.
- **Minimization** of data exposure; enclave sees minimally required data. Trade-off; data exposure to $f()$ secrecy.
- **Secrecy** of $f()$.
- Performance **overheads**.

Threat Model

- Typical SGX attacker; Compromised OS
- Untrusted Cloud, Data and Algorithm Providers
- **Software Covert Channels and Side Channels**
- Assumed run-time bug free: Intel SGX, Graphene Library OS, GUPT, Google Native Client (NaCl), Ryoan, MuJS.
- Out of scope: Hardware side channels



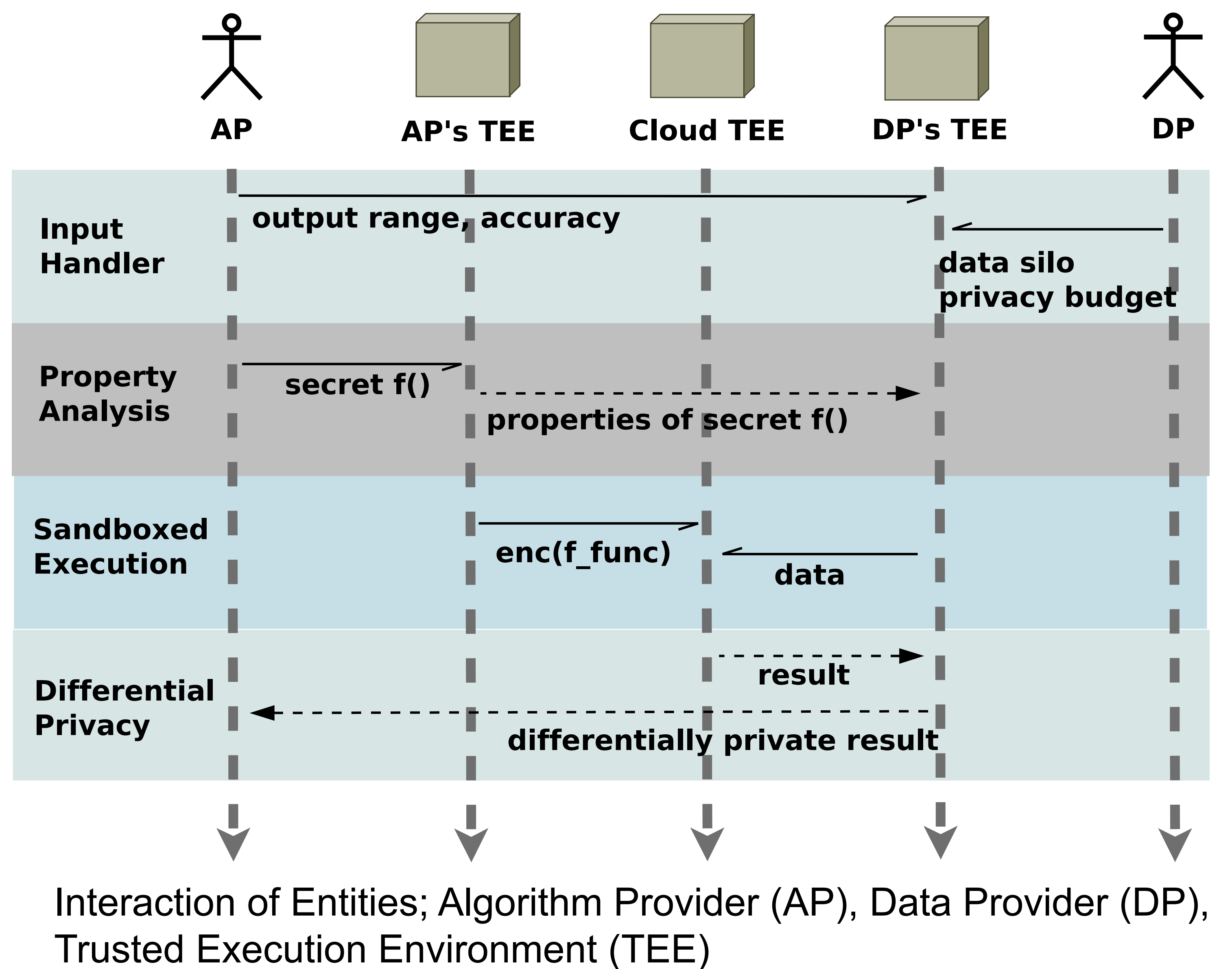
CP's TEE: Cloud Provider's Trusted Execution Environment



DP's TEE: Data Provider's Trusted Execution Environment



AP's TEE: Algorithm Provider's Trusted Execution Environment



Trustworthy Execution of Dynamically-loaded Secret Code

We propose a **system model** with **building block** approach **composes** existing solutions **securely**.

- Enabling **differential privacy** with integration of GUPT[1] (**Privacy Budget, Accuracy, Output Range**) on Graphene Library OS[5] running on SGX.
- **2-way sandbox** of Ryoan[2] & NaCl[3] on SGX for deterministic execution of encrypted JavaScript code dynamically on MuJS[4] against information leakage,
- **Property** analysis and **provisioning** of secret algorithm on SGX for **trust decisions** and **frequent updates**.

References:

- [1] Mohan et al. "GUPT: Privacy Preserving Data Analysis Made Easy", ACM SIGMOD, 2012
- [2] Hunt et al. "Ryoan: A Distributed Sandbox for Untrusted Computation on Secret Data", USENIX OSDI, 2016
- [3] Yee et al. "Native Client: A Sandbox for Portable, Untrusted x86 Native Code", IEEE Security and Privacy, 2009
- [4] Goltzsche et al. "TrustJS: Trusted Client-side Execution of JavaScript", ACM EuroSec, 2017
- [5] Tsai et al. "Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX", USENIX ATC, 2017