IOWN INTEGRAL

NTT R&D FORUM 2024
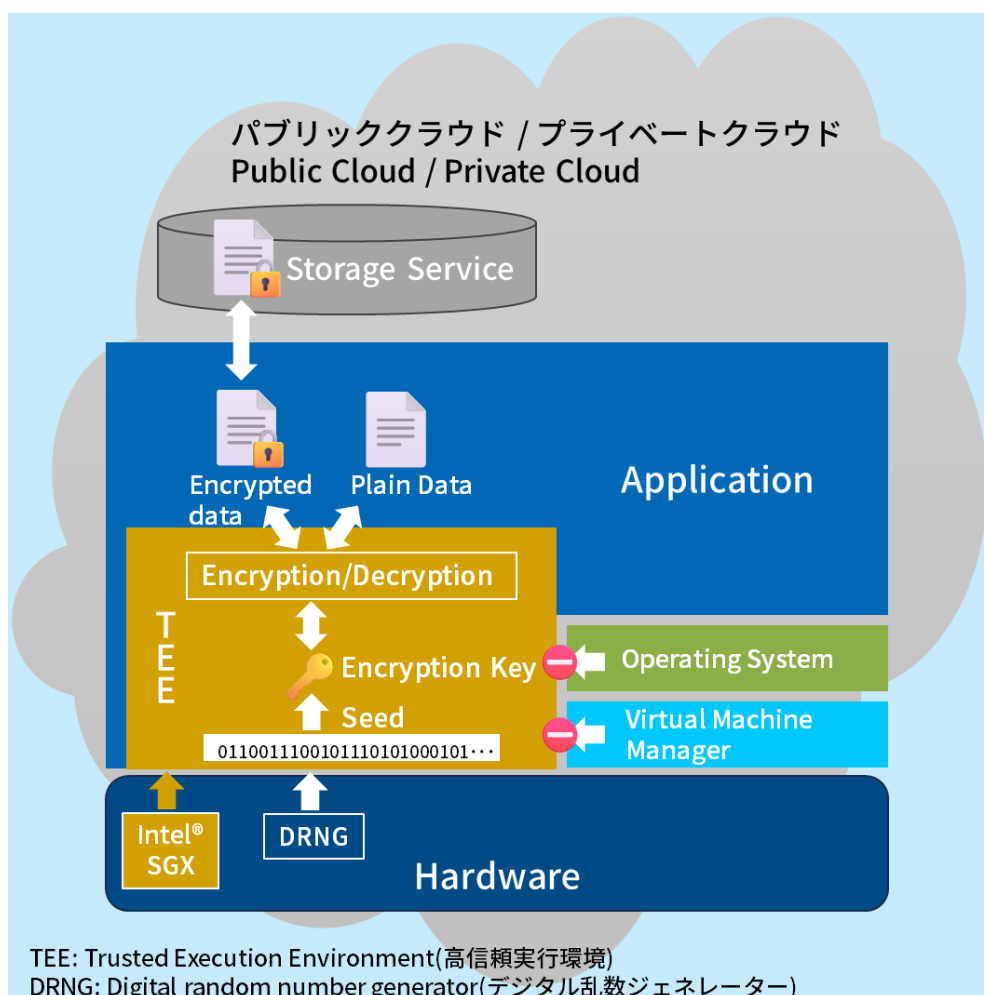
Data security technology with robust key management

Ensure confidentiality and integrity of encryption keys, and strictly protects user data

#Business Resilience

パブリッククラウド / プライベートクラウド
Public Cloud / Private Cloud

Storage Service

Encrypted data

Plain Data

Application

Encryption/Decryption

TEE

Encryption Key

Operating System

Seed

0110011100101110101000101···

Virtual Machine Manager

Intel® SGX

DRNG

Hardware

TEE: Trusted Execution Environment(高信頼実行環境)
DRNG: Digital random number generator(デジタル乱数ジェネレーター)

///Technical Issue

If cloud service provider experiences an incident in its encryption key management, such as human error or internal fraud, data security will be compromised.

///Research Goal

This technology reduces incidents related to cloud encryption key management, ensures data security, and enables safe use of cost-effective, convenient cloud services.

---Technology

- Software development know-how using TEE (Trusted Execution Environment), especially Intel® SGX.
- Knowledge gained from NTT DATA's experience using public clouds.

---Novelty

- Applicable to cloud environment to prevent leakage of encryption keys due to incidents.
- Enables scaling out of encryption and decryption. processing, achieving processing performance equal to or greater than that of existing key management systems.

---Applicable Business

Applicable to BYOE (Bring Your Own Encryption), HYOK (Hold Your Own Key), BYOK (Bring Your Own Key) on public clouds in the public, financial, and corporate sectors. (Scheduled service availability: 2026/3Q)