eperi

Your Key to your Cloud Data Protection

eperi & Intel®
Privacy Preserving Computation on encrypted Data in the Cloud utilizing Azure Confidential Computing

Dated: September 2020

TABLE OF CONTENTS

eperi GmbH
Gutenbergstrasse 4-6 / D-64319 Pfungstadt / Germany / T +49 6157 95 639 00
info@eperi.com / eperi.com

EXECUTIVE SUMMARY

Banking and capital market leaders increasingly recognize that cloud is more than a technology, it has become a destination for banks and other financial services firms to store data and applications and access advanced software applications via the internet. Banking industry leaders are focused on leveraging the cloud to drive innovation and new capabilities into their organizations.

As most companies in the financial services industry are adopting a cloud first or serverless architecture approach this presents some challenges. Data security concerns and regulatory compliance are top of mind for financial services companies and these concerns have slowed the move of private data to the cloud thus inhibiting data driving innovation.

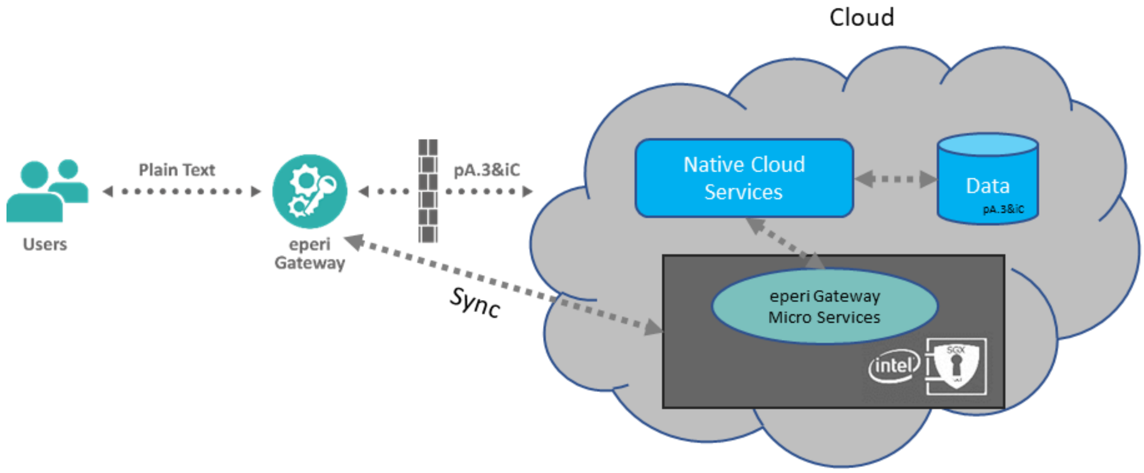
eperi has worked with a top tier bank to allow data to securely move to the cloud by encrypting data on the way out of the network using the eperi Gateway and to use **Azure confidential computing** with Intel® Software Guard Extensions (Intel® SGX) to allow computation of that data in the cloud in a privacy preserving manner, thus building a cloud based data analytics platform.

CUSTOMER CHALLENGE

The top tier bank follows a cloud-first strategy, however worldwide legal regulations e.g. GDPR or finance industry-related compliance aspects require that access to personal and business critical data is restricted in the cloud. Business departments require to aggregate data from various input channels and perform reporting and business analytics on it. One of the biggest restrictions with encrypted data is, that analytics operations cannot be performed in the cloud without having access to the unencrypted data at any point in time.

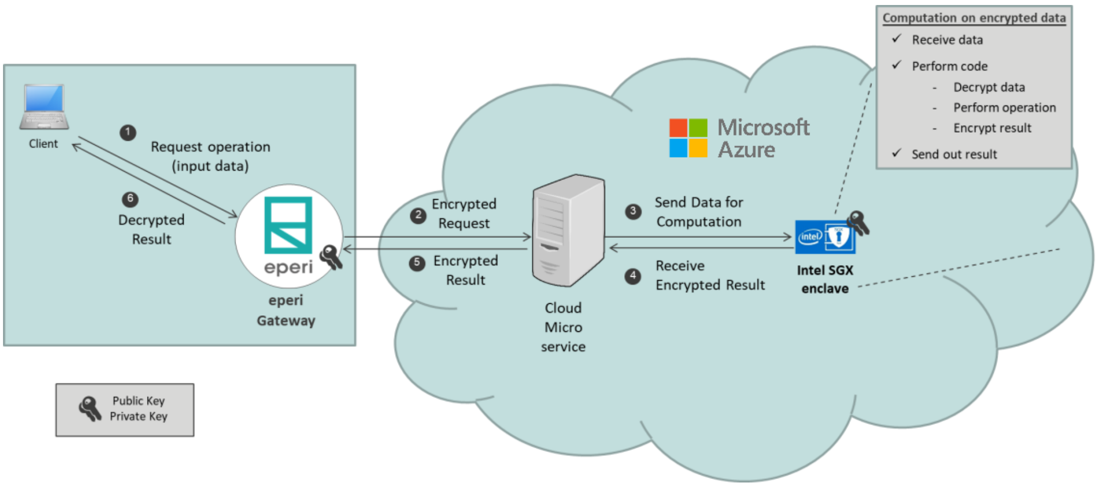
SOLUTION

The combined solution of eperi and Intel® technologies protects any type of data before moving into the cloud. The flexible template architecture of eperi’s standard product allows to protect data before it is sent to any cloud application (e.g. Salesforce or Office 365) or cloud provider. Customers and partners can create their own templates based on their security and application preferences. The Intel® SGX enclave allows security-sensitive computation of data in the cloud, while the data is protected even against operating system or virtual machine operations. eperi’s support for confidential computing allows the customer to decide which functionalities of the eperi Gateway (key management, encryption, tokenization, custom analytics algorithms) will run in the eperi Gateway on premises and which are running protected inside the Intel® SGX enclave. The eperi Gateway technology ensures that the services in the cloud are always in sync with the eperi Gateway services. With the combined solution of eperi and Intel® technologies, the restricted data is not available as clear text in the cloud at any point in time.



USE-CASE: PRIVACY-PRESERVING ANALYTICS FOR TOP TIER BANK

eperi's customer, a top tier bank, wants to share & distribute restricted data with company-internal teams, and aggregate reports and analytics based on all types of data sets. Due to legal regulations like Swiss Banking Secrecy and GDPR, the customer needs to pseudonymize data before moving them into the cloud. The eperi & Intel® SGX solution is enabling the financial institute to perform all needed privacy-preserving cloud analytics while staying compliant with laws and regulations. A proof-of-concept of eperi, Intel® SGX and the customer showed that eperi-protected cloud data can be seamlessly used for analytics operations in the Intel® SGX enclave in Azure cloud services.



SUMMARY

- ✓ The eperi Gateway ensures that all **sensitive data** will be **encrypted / tokenized** before it is sent to the cloud.
- ✓ No one is able to see the clear text data in the cloud – just the enclave is able to use the data.
- ✓ The eperi Gateway supports Azure confidential computing with Intel® SGX and allows a variety of use-cases like:
    - ✓ **All arithmetic operations and complex (analytics) algorithms** can be securely performed on encrypted data in the Intel® SGX enclave.
    - ✓ **Result data will be encrypted** before transferring to the cloud.
    - ✓ Via the **eperi Gateway** the results are displayed in clear text to the authorized client.
    - ✓ The customer solely **stays in control** of their critical data.
    - ✓ The customer **complies** with all international compliance requirements for data security in the cloud.
- ✓ **Analytics operations for high-secured data** can be performed with eperi & Intel® SGX combination.
- ✓ **Cloud data** is **useless** to any attackers, any externals, the cloud provider or eperi.

ABOUT EPERI

eperi is a leading player in the IT Security sector, with many years of experience in the field of data encryption for cloud applications. eperi is listed in six Gartner Hype Cycles. eperi is headquartered in the Greater Frankfurt area, in Germany and holds several global patents for its innovative technology, providing unrivaled data protection for databases, applications, and file storages.

eperi's solutions deliver data-centric security such as field level encryption, tokenization and unstructured data encryption when using cloud services, web applications and private apps from anywhere, on any device. eperi works together with some of the world's largest and well-known organizations in the finance, healthcare, and industrial sectors to empower them with GDPR compliance, solve data residency problems, and fulfill legal requirements. It also enables its customers to take full advantage of the Cloud without having to worry about data security, compliance, and liability irrespective of the cloud application they use. More Information on www.eperi.com.

ABOUT INTEL®

Intel® SGX is designed to ensure application integrity and confidentiality, protect execution and help keep the data protected. The hardware-based enclaves are encrypted to help to protect sensitive information and data by creating a trusted space where new CPU instructions provide higher security access controls and execution. This helps to keep the most important information confidential, unmodified and secure while it's in use in memory. When the enclave is launched the integrity of protected software and data can immediately be verified, helping to ensure that the data being protected is free of modification. In today's multitenant clouds, threats can come through the underlying platform, from a virtual machine hosted on the same server or even from a compromised application inside the VM. Intel® Software Guard Extensions provides the technology for building security solutions that help to safeguard your applications and businesses most sensitive data. More information about Intel® SGX on **www.intel.com/sgx.**

Intel, the Intel logo and Intel SGX are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries