eperi & Intel® - Confidential Computing on a new Level

Privacy Preserving Analytics on encrypted Data in the Cloud utilizing Azure Confidential Computing

Dated: December 2020

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

AT A GLANCE

- ✓ 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 in the secure Intel ® SGX enclave the data can be used with the eperi Gateway Micro Services.
- ✓ **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.

More and more companies – even in highly regulated industries – adopt a cloud-first and serverless architecture approach. But this process is slowed down by data security concerns and the need to comply with legal regulations.

With the eperi Cloud Data Protection Solution combined with Intel® Software Guard Extensions (Intel® SGX), Confidential Computing is brought to a new level. Sensitive data is protected in the cloud at any time – even while running analytics on this protected data.

CHALLENGE

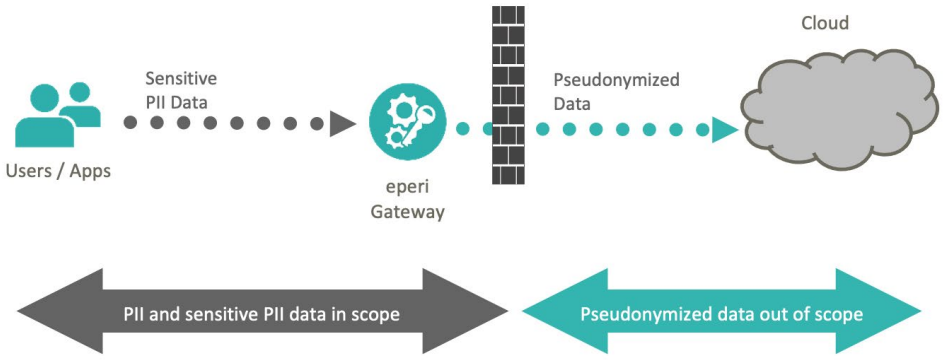
Organizations across all industries started to realize the economic potential of their data repositories. Much of this information contains personal data. The privacy risk for the associated individual is only carried by the organization, as they are in sole legal responsibility for the data.

Regulatory requirements on privacy and on data protection are strengthened globally. Non-compliance leads to considerable risks. Developing capabilities to analyze data are massively growing and drive a demand for new technologies to preserve privacy during analytics and business intelligence processes.

eperi has worked with a top tier bank to allow them building a cloud-based data analytics platform while worldwide legal regulations require that access to personal and business critical data is restricted. This top tier bank faced the challenge that their business departments require to aggregate data from various input channels and perform reporting and business analytics. As most of these data are Personnel Identifiable Information (PII), they needed a solution that is able to pseudonymize and encrypt the data while it is protected even during the analytics processes. But one of the biggest restrictions with pseudonymized and encrypted data usually is, that analytics operations need to be performed on unencrypted data at any point in time. A no-go in the cloud!

SOLUTION

Pseudonymization and encryption with the eperi Gateway enables companies to securely use the public cloud, while maintaining information value. This is the key for Privacy Preserving Analytics. According to worldwide laws, anonymized and correctly pseudonymized (de-facto anonymized) data is descoped from the data protection laws as it is not seen as Personal Identifiable Information (PII).[1]



The eperi Gateway employs a variety of capabilities to transform personal data and as such provide a balance that satisfies corporate utility and personal privacy. It reduces the sensitivity levels of personal data, or even renders it (temporarily) anonymous – "on the fly", in real time. As a proxy acting transparently in the data stream, it was built to be completely invisible for both the user and the cloud application. It's a quick-to-set-up solution enabling compliance to pressing regulatory requirements.

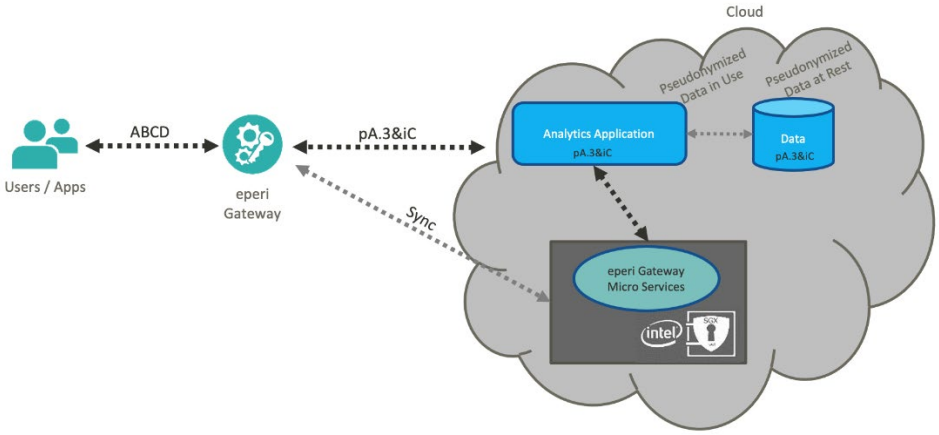
The eperi Gateway is the only solution in the world, that supports hybrid multi-cloud environments. Cloud Providers build "distributed clouds" to provide services at the point of need, giving customers new opportunities with anywhere operations. Only "the cybersecurity mesh enables anyone to access any digital asset securely, no matter where either is located" as also Gartner stated in their Top Strategic Technology Trends for 2021. In the same report, "Privacy-Enhancing Computation" is seen as a Strategic Technology in 2021 and Gartner assumes that by 2025, 50% of large organizations will adopt it. Privacy-Enhancing Computation "provides a trusted environment in which sensitive data can be processed or analyzed. It includes trusted third parties and hardware-trusted execution environments (also called Confidential Computing)."

Additionally to common data-at-rest security controls, the eperi Gateway protects data in use, thus enabling the use of the data, while maintaining secrecy or privacy.

The combined solution of eperi and Intel® technologies protects any type of data before moving into the cloud. This enables organizations to implement data processing and analytics capabilities that were previously impossible because of privacy or security concerns.

The Intel® SGX enclave – as a secure hardware execution environment - allows security-sensitive computation of data in the cloud, while the data is protected even against operating system or virtual machine operations. Said in simple words: Confidential Computing makes it possible to run operations with data on somebody else's computer but where the owner of that computer can neither influence nor observe what's happening.

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 or in the public cloud 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 public cloud at any point in time.



As described in the diagram above, authorized users or applications work with the critical data in clear text. The eperi Gateway pseudonymizes the critical data before it is sent to the cloud. This ensures that the cloud provider or even attackers are unable to use the stolen data as it is pseudonymized. All the connections to and from the eperi Gateway are of course transport encrypted, enabling a "Data in Transit" security. Inside the analytics application (Data in Use) as well as in all the data lakes and storages (Data at Rest) the data is pseudonymized.

The former downside of pseudonymized data - that operations can´t be performed on these data - has been solved with the help of the eperi and Intel® solution. Analytics applications trying to perform operations on pseudonymized data are enabled by the eperi Gateway Micro Services in the Intel SGX® enclave to perform these operations in a reliable and secure environment.

The unique eperi Gateway Technology ensures that the eperi Gateway is constantly synchronized with the eperi Gateway Micro Services running in the secure Intel® SGX enclave.

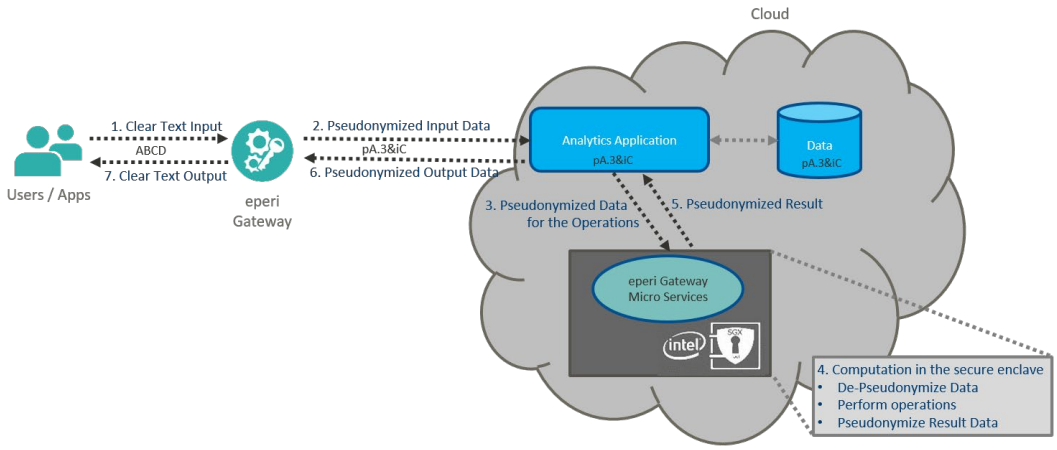
This allows customers to perform all analytics operations they want on pseudonymized data without having to worry about security and privacy.

SOLUTION DETAILS

The eperi & Intel® SGX solution is enabling the financial institute to perform all needed cloud analytics in a privacy-preserving manner and to stay compliant with laws and regulations worldwide. Already during the proof-of-concept phase eperi was able to show that eperi-protected cloud data can be used seamlessly for analytics operations in the Intel® SGX enclave in Azure cloud services.

As many new security trends - like homomorphic encryption - have a very limited operation area and unproven security level, this joint solution is outstanding.

Customers are free to use their own crypto algorithm to secure the data (Crypto Agility) based on their company internal security policy – HSMs, Multiparty Computation or Post Quantum Crypto Algorithms can be used. This enables the use of the best and most trusted encryption and tokenization algorithms. Additionally, with help of the Intel® SGX enclave, all operations on secured data can be performed seamlessly. This future-proof solution offers everything that is needed today and that will be needed tomorrow.



The diagram above shows the workflow that enables privacy preserving analytics.

1. The authorized user or application sends the input for the analytics application / ETL-Tool in clear text as usual. As a reverse or forward proxy in the data-stream, the eperi Gateway pseudonymizes the critical data when the clear text data is sent across. Technically, pseudonymization is a combination of encryption and tokenization. The huge advantage of the eperi Gateway is, that there is neither need for an installation on the user side, nor on the application / cloud side.
2. The pseudonymized data are then sent to the analytics application, which is able to work with this data and e.g. store it in a data lake.
3. If the analytics application needs to perform operations on the pseudonymized data, it calls the eperi Gateway Micro Services running in the secure Intel® SGX enclave.
4. The eperi Gateway Micro Services de-pseudonymize the data. On the clear data any operations can be run. The result is pseudonymized again. During the operations, the secure Intel® SGX enclave ensures, that no administrator, no attacker, no operating system or virtualization system is able to access the data in clear text. As Intel® moved the SGX functionality into the mainstream server processors starting with the “Sunny Cove” cores in the Ice Lake Xeon SP Processors, all this happens on hardware level. Xeon E3 processors from 2015 through 2018, and the Xeon E series from 2019, support SGX, too. The SGX enclave coming with Ice Lake Xeon SPs will support up to 1 TB of application and data.
5. The pseudonymized result is then transferred back to the analytics application in the cloud and can be processed, e.g. stored there.
6. As soon as the authorized user requests the data, it is sent via the eperi Gateway where it is de-pseudonymized.
7. The authorized user receives the data in clear text format. This complete process works transparently for the user who is able to use the integrated app functionalities with no need for any additional plugins or adapted workflows on the user side. The clear text data is unveiled at no time to the cloud provider or the analytics application.

The following example shows the process from the analytics application perspective. The encrypted request with the pseudonymized data is sent to the Intel® SGX enclave where it is de-pseudonymized and the (in this example simple) operation is performed. “10237123 + 2923740 + 234250 + 1683677951 = 1697073064” The result is then pseudonymized again and sent back to the Analytics Application transport encrypted.

Encrypted request data protected by eperi is sent to the Intel® SGX enclave.

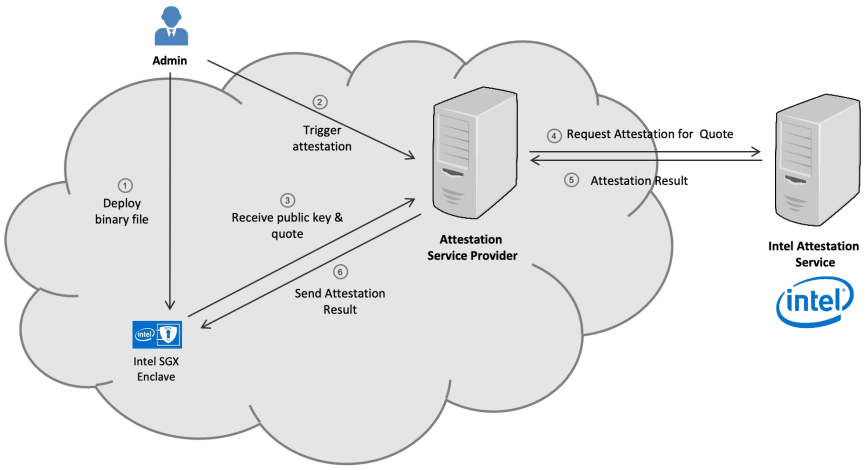
eperi Gateway Micro Services are performed in the Intel ® SGX enclave:

- ✓ Decrypt data / De-Pseudonymize values
- ✓ Perform operation
- ✓ Pseudonymize values / encrypt result

Encrypted result is received in the Analytics Application.

One of the major security anchors is the trustworthiness of the executed code inside the Intel® SGX enclave. Therefore, the initialization of the enclave is done with the code and the encryption key. The process is described in the following and shown in the schema:

1. The administrator of the company who uses the eperi Gateway deploys the eperi Gateway Micro Services as binary file to the Intel® SGX enclave.
2. He also triggers the attestation service provider,
3. who receives a public key and a quote from the Intel® SGX enclave.
4. The attestation service provider sends the request for an attestation for the quote to the Intel attestation service, which
5. returns the attestation result to
6. be send to the Intel® SGX enclave.



RESULTS

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 / tokenized** before it is transferred back to the cloud.
- ✓ Via the **eperi Gateway,** the results are displayed in clear text to the authorized user.

- ✓ The company (data owner) solely **stays in control** of their critical data.
- ✓ The company **complies** with all international compliance requirements for data security in the cloud.
- ✓ Cloud data is **useless** to any attackers, any externals, the cloud provider as well as eperi.

LEARN MORE

The joint eperi and Intel® solution is mainly used for Privacy Preserving Analytics in the Cloud.

The eperi Gateway can be implemented for a variety of cloud applications like Microsoft 365/Microsoft Teams as well as Salesforce and custom applications. This allows customers a secure and legal compliant usage of all could applications.

To learn more about the various possible uses of the eperi Gateway please visit the following pages:

- ✓ Microsoft Teams
- ✓ Microsoft 365
- ✓ Salesforce

SPOTLIGHT ON EPERI

eperi is on a mission to enable companies to regain full control over their data, regardless of where the data is stored. eperi's software solutions deliver unrivaled data-centric security empowering customers 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 – and all this without the Cloud-Provider gaining control over their data.

The leading player in the IT Security sector is headquartered in the greater Frankfurt area, in Germany, and provides many years of experience in the field of data encryption for cloud applications. eperi holds several global patents for its innovative technology and is listed in six Gartner Hype Cycles.

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. Some of the world's largest and well-known organizations in the finance, healthcare, and industrial sectors use the eperi Gateway to be empowered with GDPR compliance, solve data residency problems, and fulfill legal requirements. eperi 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.

[1] "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." Recital 26 (5) GDPR

[2] For purposes of data security and client confidentiality, our customer asked us not to disclose their name. But they agreed we could share the story of their success working with the eperi Gateway and Intel® SGX.