Privacy enhancing computation

Definition

**What is Privacy-Enhancing Computation?**

Falling under the category of “people centricity,” [Gartner](https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/) defines PEC as featuring three technologies that protect data while it is in use. These technologies include:

* A trusted environment where sensitive data can be processed or analyzed.
* Performs processing and analytics in a decentralized manner.
* Encrypts data and algorithms before analytics or processing.

PEC is designed specifically for the increasing need to share data while maintaining security or privacy. The main purpose of PEC trend is to encrypt data that is processed on the third-parties hardware

**Why Trending**

Global data protection legislation is maturing and, with the unstoppable pervasiveness of personal data, every organization that processes personal data faces ever-higher privacy and noncompliance risks. At the same time, organizations now realize the economic potential of their data repositories.

The demand for processing data in untrusted environments and performing multiparty data sharing and analytics is rapidly growing. The increasing complexity of analytics engines and architectures mandates a by-design privacy capability, rather than a bolt-on approach. Unlike common data-at-rest security controls, privacy-enhancing computation protects data in use, thus enabling the use cases described previously, while maintaining secrecy or privacy. As a result, organizations can implement data processing and analytics that were previously impossible because of privacy or security concerns.

**Privacy-enhancing technologies**

The privacy-enhancing computation trend involves a range of different modern technologies that aim to protect personal data in various methods.

1. **Homomorphic encryption**

This technology lets computation on encrypted data for third-party providers. It means that the data will be confidential but can be processed. As we mentioned above, people`s private data is used in many spheres like medical, banking, working, etc. Homomorphic encryption provides the ability to process this data by a general index without the need for private information. Thus, a required part of data can be unencrypted only by those who have the particular keys to access for performing different computations on it.

1. **Trusted execution environments**

A trusted execution environment or TEE is a safe environment for the main device separately from the operating system. It provides a high level of protection for data while it is being stored or processed. TEE applies the function of trusting or not your device to other devices, to allow or forbid access to the location, photo gallery, and other data for third-parties providers and other applications. It also can ask for a password, authentication code, email or phone verification, etc.

1. **Multi-party computation**

Multi-party computation is a cryptographic protocol that allows analyzing various data without violating privacy. It means the data from several parties can be distributed and analyzed, and no party cannot see the initial data.

1. **Differential privacy**

Differential privacy is an algorithm that analyzes data and generates its statistics. It hides the individual data and shows the general dataset. The algorithm almost does not change if an individual joins or leaves the dataset. It guarantees the protection of individual-level information.

**Personal data stores**

A personal data store (PDS) is general access to individual data and the ability to upload, share, change, or delete this data by the data owner. It can contain addresses, phone numbers, passport data, bank accounts histories, electronic health records, etc. This technology enables controlling own data by each individual. A personal data store aims to provide the opportunity to add or take out the private data on the third-party providers’ side. This type of stores has a range of benefits for a business like:

* more effective gathering and keeping data
* absence of law risks to announce private data without permission
* the data can be easily updated

Our developers are experienced specialists with advanced skills and easily can find the appropriate solution for your business company to protects private data. They know how to accurately [implement privacy-enhancing technologies](https://gbksoft.com/contact) to make the data protection processes more effective for your project.

**PETs use**

As all privacy-enhancing technologies were counted above, we would like to discuss where these technologies are used and what functions they perform to protect users` private data.

1. Anonymizers

This tool is related to users` behavior on the web. Its main aim is to hide the real geolocation, email, and other information about users. It is not also hidden but replaced by inexisting data like accidental emails, nicknames, IP addresses. It can perform for one website, mail, messenger as well as for the browser.

1. Fake accounts

This method is usually used when a user wants to create an account on a specific website or apps and doesn’t want to show the real personal information. Such users create fake emails, use false names and contacts, fictional bio, interest, etc. These bogus accounts can also be used for more serious aims than social media. It adds the user to a particular system but doesn’t show the real data.

1. Confusing data

Confusing private data is one of the good practices to protect it. The account can be real and contains true information. Along with it, users can add mixing-up facts and distracting data elements. This method hides the personal real information with masking techniques and specific algorithms. So in case of a hacker attack, it will be much more complicated to recognize the required data.

1. Private data access

This example applies differential privacy technology. Each individual has constant access to their data, can change, update and delete it at the user’s own discretion. It means that some data disappears forever and can not be kept or used anymore.

1. EPID

This is a kind of digital signature that is created to identify the group or system members without showing who it is. The key is usually complex and consists of several verification steps.

1. Pseudonymization

This technique aims to identify private data with pseudonyms and hide the real content. It does not influence data analysis or data processing. It is used to cover the individual as well as group information.

**Examples of PEC Applications**

The ability to leverage datasets to which you don’t have access opens up a world of possibilities in terms of applications. Here are just a few examples:

**1.      Fraud prevention**

Fraudsters tend to specialize in and target multiple companies within specific industries. By leveraging PEC, companies can catch these fraudsters quickly. Further, they can identify good customers if they’re collaborating with one another to create a pool of trusted identities without sharing any personal user data.

**2.      HR**

If you work for a company that is looking to minimize the gender pay gap, you can use PEC to work with other companies in your industry and measure the situation with real data. Of course, that’s just one example, but the opportunities for data analysis are truly an exciting frontier.

**3.      Internal data analysis**

PEC can help you perform data analysis without worrying about sharing data between brands or across different regions, such as from the U.S. to the EU. PEC gives companies the opportunity to collaborate with competitors or across borders, leveraging data directly, leading to better results thanks to more recent data.

**4.      Medical research**

Many regulations rightfully protect patient data. However, medical research often needs to be able to gain insights from data across laws and borders. With PEC, this process becomes much easier and privat

Future

Gartner predicts that by 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments or multiparty data analytics use cases.