Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Published 28 June 2021 - ID G00743768 - 15 min read

By Analyst(s): Bart Willemsen, David Mahdi, Mark Horvath

Initiatives: Technology, Information and Resilience Risk

Privacy concerns have led to constraints around how and where personal data is processed. Security and risk management leaders can manage constraints while respecting individual privacy by applying PEC techniques in AI modelling, cross-border data transfers, and data analytics.

More on This Topic

This is part of 2 in-depth collections of research. See the collections:

- Where Next? Technology Leadership in a World Disrupted: Key Insights From the 2021 Gartner IT Symposium/Xpo Keynote
- Applying AI — Governance and Risk Management

Overview

Impacts

- The use of identifiable and regulated data for artificial intelligence (AI) model training raises compliance concerns around personal data usage and potential negative effects in production deployments.
- An increase in international restrictions on cross-border data transfers amid ongoing cloud adoption leaves stakeholders confused and hesitant about their cloud and infrastructure strategy.
- Restrictions from various regulations on the use of personal data, as well as customer demand for privacy, inhibit opportunities to share, pool and/or analyze such data.

Recommendations

Security and risk management (SRM) leaders with a focus on privacy, technology, information and resilience risk should:

- Treat privacy risk in AI model training by applying differential privacy and/or synthetic data to protect identifiable data, and federated machine learning (ML) to enhance privacy across training stages.
- Protect personal data from being accessed by unauthorized entities by using confidential computing, or secure enclaves, either from a third party or OEM from the service provider itself, where the key management architecture allows it.
- Use a combination of privacy-enhancing computation (PEC) techniques to keep data and/or algorithms secure during data processing and analytics. Understand that the capabilities and techniques required may vary greatly depending on whether the use case is an internal or external one.

Strategic Planning Assumption(s)

By 2025, 60% of large organizations will adopt PEC for processing data in untrusted environments and multiparty data analytics use cases.

By 2026, 40% of data repositories, such as data lakes, will include native capabilities for PEC, up from less than 5% today.

Introduction

Disclaimer: While Gartner research may include reference to related legal issues, we do not provide legal advice or services, and our research or guidance should not be construed or used as a specific guide to action. We encourage you to consult with your legal counsel in considering and applying the advice and recommendations contained in our research.

PEC techniques feature in Gartner's Top Strategic Technology Trends for 2021. Many individual PEC techniques are briefly described in Gartner's Hype Cycle for Privacy, 2021. Though PEC is a group term, there is benefit from using these techniques in specific combinations for different use cases. They can be applied on different levels (see Figure 1). Data can be transformed, either in place (encryption), or in a new repository (synthetic data) or on the fly (differential privacy). On the software or compute level, additional safeguards can be added, and even on the hardware level there are options to isolate environments securely. Ideally, selecting techniques on multiple levels in combination provides more robust protection.

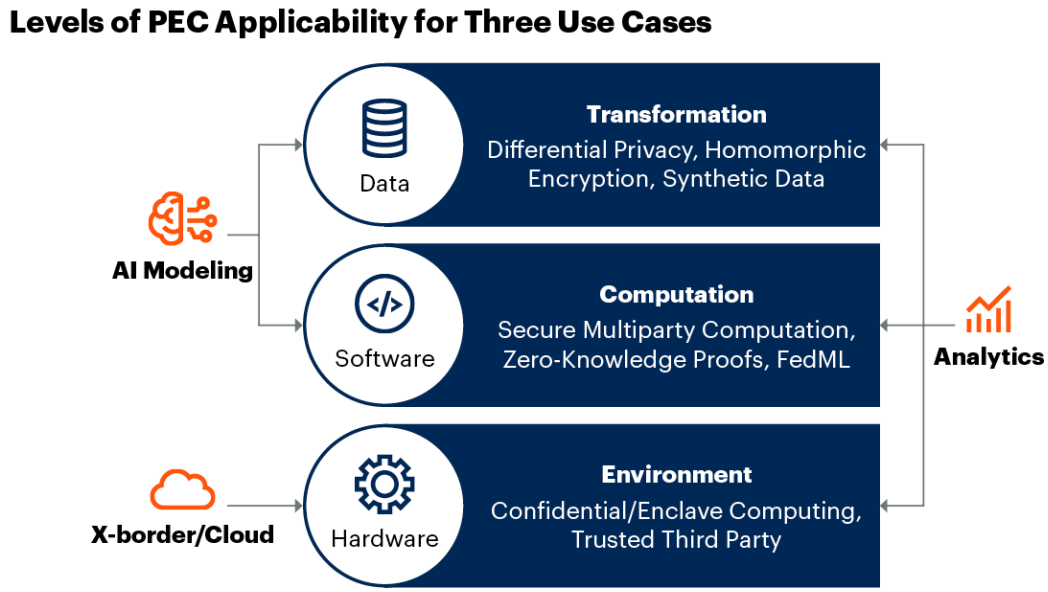
This note describes three key use cases with applicable PEC techniques:

1. AI model training and sharing models with third parties.

2. Usage of public cloud platforms amid data residency restrictions.

3. Internal and external analytics and business intelligence activities.

Figure 1: Levels of PEC Applicability for Three Use Cases



Source: Gartner
743768_C

Gartner

Impacts and Recommendations

Usage of Personal Data in AI Model Training Raises Compliance and Ethical Concerns

Bias and discrimination in decision making, if left unchecked, are amplified in automated AI use cases. Unethical use of personal data is further undermining trust in AI, not to mention fears — justified or not — about future AI being a threat to employment and society at large. At the same time, AI has proven to be a very powerful toolbox to help solve many of today's great challenges in business, healthcare, safety, security and welfare. Furthermore, many modern privacy and data protection laws require "purposeful processing" of personal data (for more information, see Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria). Training algorithms and AI models with directly identifiable data can lead to processing such data outside transparently conveyed purposes. Operational deployment can sustain bias for lack of diversity, and have an operational impact on the actual individuals whose personal data was trained on if they remain identifiable.

Moreover, with legislative efforts increasing to further govern the creation, offering and use of AI, the pressure on SRM leaders increases to ensure responsible, explainable, transparent and nondiscriminant use of AI technology. Although using AI responsibly is also a matter for nontechnology executives (see What Non-Technology Executives Should Do in Support of Responsible AI Initiatives), SRM leaders should lead by example and continue business enablement by investing in PEC techniques to proactively protect personal data, thereby preventing compliance issues and other privacy concerns from arising.

Ideally, a combination of PEC techniques on different layers adds to the effectiveness of the protection framework. In this case, SRM leaders should focus both on the data and on the software level.

SRM leaders must first choose how to treat data before determining how to use it for training.

- In simple setups, especially when the data used for training resides in a single repository or can be static, SRM leaders should investigate the use of **synthetic data** from generative AI (see Innovation Insight for Generative AI). The algorithms can be trained on a synthetic dataset, which represents no single individual and can be balanced to contain the desired diversity of content. In short, synthetic data helps to:
  - Augment training data to build AI models when insufficient data is available.
  - Protect privacy, as synthetic data resembles real data but cannot be traced back to a person.
  - Reduce bias by using generated data to balance training data.
- When multiple data sources are in play, making the source data available through **differential privacy** may be a better choice, which prevents the need to create large new repositories of data, using the original sources. This also allows for periodic adjustment, as the source data may change over time (trend analysis) but needs no alteration at the source, since differential privacy treats the data "on the fly" while it's being queried or made available.

At the application level, **federated machine learning** (FedML) enables local learning by training and retraining ML models in a decentralized runtime environment — without the need to share local data centrally or in a common runtime environment. Learning models can be transferred without having to copy or transfer the data at all. Local learning may occur in smartphones, softbots, autonomous (or semiautonomous) vehicles or IoT edge devices.

In addition, FedML enables collaborative learning by sharing local model improvements at a central level. This feedback is then used to generate a new, improved common model that may be deployed (or redeployed) to decentralized or local runtime environments. FedML provides the capability to train models on each device and in each repository, and across competing or otherwise separate entities, using the data captured on the server, database or (edge) device. The trained models are transferred to the server and merged or averaged together to create a model that captures the patterns in the data on all the edge devices.

International Restrictions on Cross-Border Data Transfers Bring Confusion and Hesitation to an Organization's Cloud and Infrastructure Strategy

Major jurisdictions like China and Russia put specific restrictions on data not to be sent out of the country. India may soon follow with the pending enactment of the Personal Data Protection Bill (PDPB). Whether law or preference, an increasing number of countries seem to want to put restrictions on cross-border data transfers. Since the "Schrems II" ruling of 16 July 2020, the topic of data residency has also become a critical consideration for organizations operating in member states of the European Economic Area (EEA) and has since been extended with a focus on confidentiality concerns using various forms of cloud computing.

A key technology here, mainly applicable for infrastructure as a service (IaaS) and platform as a service (PaaS) scenarios, is **confidential computing**:

- **Confidential computing** allows the storage of data or execution of code to take place in a hardware-based trusted execution environment (TEE), also called a **(secure hardware) enclave**. Enclaves isolate and protect code and data from the host system, as well as from the host system's owners, and are sometimes also used to provide code integrity and attestation assurance.

Some cloud providers offer use of confidential computing as part of the OEM offering. This will depend on several factors such as: your own risk assessment; the level of trust granted to the service provider; your risk appetite, whether or not the mechanism of the cloud provider is used; and if an independent provider is preferred. Note that if you rely on encryption key management to ensure that confidentiality is maintained, the encrypt/decrypt operation should take place where it is unreachable by the cloud provider, and the key is held in a tenant within the jurisdiction where the residency restrictions apply. SRM leaders need to always combine confidential computing with an appropriate encryption method and key management architecture (in isolated control).

Regulatory Restrictions and Customer Demand for Privacy Inhibit Opportunities to Share, Pool and/or Analyze Personal Data

Primary processing purposes are often simply served by identifiable information within the parameters of legal requirements and customer expectations. For (cross-entity or stand-alone) analytics and business intelligence use cases, personal data usage does not often pass the tests of proportionality, subsidiarity and purpose limitation. Data scientists do not have access to the same (identifiable) information as their operational colleagues, and organizations can't just send data everywhere for reasons of confidentiality, be it following privacy restrictions or confidentiality requirements pertaining to intellectual property. One main differentiation for determining which PEC technique(s) to use is in whether the control should be internal or external.

Internal

One can imagine that, when both the lock and the key are under guardianship of the same entity, it is difficult to maintain that data was not easily reidentified. Providing data scientists with a pseudonymized or partially encrypted copy of the CRM database is not a direct solution. After all, based on the completeness of a record on attribute level, the data scientist, in theory, can just cross the corridor to, say, the customer care service department and retrieve the identity of the person behind the data.

Two main PEC techniques resurface: **differential privacy** and **synthetic data**. One of the main differences between these is whether or not there is a need to establish a fixed subset of data in a separate repository. Synthetic data is generated using different methods such as statistically rigorous sampling from real data, semantic approaches or by creating simulation scenarios where models and processes interact to create completely new datasets of events.

There is a risk that synthetic data itself adds a certain bias, so continuous statistical testing is required to ensure appropriate content representation. Using generative AI to create balanced, synthetic data allows for a consistent set of analyses to be conducted over a longer period of time where the (synthetic) dataset remains the same.

Differential privacy, instead, may allow for more trend analyses over time. Where synthetic data reproduces a static new dataset, differential privacy does not alter the underlying data. Instead, alterations to protect privacy are made in between the data at the source, and the final answer to any data scientist's query. In essence, differential privacy allows access to information, while withholding or distorting certain information elements about individuals in the dataset. Through use of mathematical algorithms that keep track of reidentifiability risks versus information value maintained, certain noise is ingested, randomization applied and linkability prevention calculated to ensure that the resulting query answer does not significantly change whether the individual's data is included or not. In combining the allowed query opportunities with **privacy-aware machine learning** (PAML), the resulting answers can be curtailed by predetermined thresholds (e.g., minimizing the number of individuals represented in an answer) and prevent query stacking (to avoid risk of singling out individual records).

External

A good few PEC techniques can be relevant in external use cases. The obvious benefits from both synthetic data for sharing, or making the data available through differential privacy to external querying entities, require no repetition here.

One opportunity lies in the use of **zero-knowledge proofs** (ZKP), which is essentially a privacy-preserving messaging protocol. It allows two organizations to verify whether information assumed to be available to both of them is correct, without sharing or transferring that exact information (e.g., for age verification without using date of birth). Rather than just focusing on an entity (prover) who tries to persuade the receiver (verifier) that the information is accurate (either false or true), the goal is to also address the issue of a verifier learning more about the information than merely if it is accurate or not. This challenge has applicability in a wide range of use cases, especially in the context of authentication and transaction verification. Other cases include payments, custody management, anti-money laundering (AML)/know your customer (KYC), consumer identity access management (IAM), medical records, and mergers and acquisitions.

Subtypes of ZKP include **private set intersection** (PSI) and **private information retrieval** (PIR). Using PSI, two entities can compare encrypted versions of the datasets each holds in order to compute the intersection of the data. As a result, neither entity reveals anything to the other entity in terms of content, or identifiable data, except for the elements on where the intersection of data takes place. PIR, on the other hand, allows data to be accessed while it's kept in an untrusted environment. A PIR protocol allows an individual to "retrieve" an item from a location where a database sits, without revealing which item is retrieved. PIR is sometimes referred to as aversion or a subset of "1 out of n" (oblivious) transfer, where it is also required that the user should not get information about other database items.

At scale, with regard to financial information on AML across financial institutions, or health information in the COVID-19 response across healthcare providers, we see an opportunity for **secure multiparty computation** (sMPC).

sMPC pertains to distributed computing and use of cryptography that enables entities (organizations, applications, individuals or devices) to work with data while keeping either that data, or encryption keys, in a protected state (or both). Specifically, sMPC allows for multiple entities to share insights using data protected in use. One can envision data being transformed across multiple entities who wish to contribute, before it leaves the controlled environment, and centrally pooled in, for example, a **trusted third party** (TTP) environment. Keys are semi-randomly cut in parts, where the components are distributed across all contributing entities and, as a result, none can decipher anything other than what was already known to them. Upon receipt in the TTP, data can be treated once more and the use of **homomorphic encryption** (be it partial, fully, or over the Torus) allows computation on that data while it remains in a protected, encrypted state. Coincidentally, even the applied algorithm can benefit from running in an equally encrypted state.

Homomorphic encryption is a set of encryption algorithms that enable computations on encrypted data. Fully homomorphic encryption (FHE) supports arbitrary mathematical operations, but has significant performance impact and is not yet applied much. Further innovation is needed to make this more practical. Partial homomorphic encryption (PHE) supports much more limited use cases with lower performance impact than FHE. Currently, commercial products are supported by some versions of PHE, but fast FHE over the Torus (TFHE) is beginning to appear in the market and has made significant performance improvements. As such, it can be combined with sMPC for robust protection. Organizations can transform the identifiable data, send it to others for processing and return accurate results without fear that the data will be lost, compromised or stolen. Any data intercepted by a malicious actor will be encrypted and unreadable, even by the coming generation of quantum computers.

Evidence

[1] The EU's efforts to regulate AI are broad in nature — see Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts: COM/2021/206 Final.

In the U.S., the Federal Trade Commission (FTC) calls for similar control on fairness, equity and truth(fulness) — see Aiming for Truth, Fairness, and Equity in Your Company's Use of AI.

[2] General cross-border transfer restrictions can be found in:

- Article 37 of the Cybersecurity Law of the People's Republic of China, which requires critical information infrastructure operators to store personal information and important data generated from critical information infrastructures in China.
- The Draft Data Security Law of the People's Republic of China, which was revised by the National People's Congress of the People's Republic of China. For an unofficial translation, see Translation: China's "Data Security Law (Draft)," New America.

Additional provisions are to be put forth in expected revisions of China's Civil Code, which is to contain a chapter dedicated to privacy provisions.

[3] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions), the Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media.

[4] The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.

[5] In client inquiries, Gartner sees similar restrictions signaled from regions including Thailand, Morocco, the UAE, Uganda and Malaysia.

[6] The CJEU Judgment in the Schrems II Case, European Parliament.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Predicts 2021: Balance Privacy Opportunity and Risk

Move to Contextual Privacy in Digital Society

Preserving Privacy While Using Personal Data for AI Training

Top Strategic Technology Trends for 2021

Hype Cycle for Privacy, 2021
