Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

Published 18 October 2021 - ID G00755920 - 11 min read

By Analyst(s): Bart Willemsen, Ramon Krikken, Mark Horvath

Initiatives: Technology Innovation

The globally expanding pressure to protect privacy and data confidentiality demands that IT leaders investigate and invest in privacy-enhancing computation (PEC) techniques. PEC provides robust, sustainable measures to gain, pool, process or share information while data remains protected in use.

Additional Perspectives

- Summary Translation + Localization: Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation
  (14 December 2021)

Overview

Opportunities

- Privacy-enhancing computation (PEC) techniques allow protection of data in use, in addition to conventional approaches for in-transit and at-rest protection. It supports processing of data confidentially in analytics and business intelligence, using untrusted computing environments like public cloud, and enabling data monetization and privacy protection scenarios that were not possible with previous approaches.
- "PEC" is an umbrella term for various forward-looking and emerging techniques — each with different security and privacy guarantees. They can be used individually, but may also be combined for greater assurance. The exact choice of techniques depends on the use case at hand.
- PEC techniques have matured to the point where commercial implementations are increasingly available. Hyperscalers are adding trusted execution environments to their IaaS offerings, and other vendors offer similar protection stand-alone. Secure multiparty computation and homomorphic encryption products are available from an increasing number of vendors. The applicability of differential privacy and synthetic data is becoming commonplace in AI model training and analytics use cases.

Recommendations

IT leaders with a focus on technology, innovation and privacy:

- Determine which PEC techniques mitigate privacy risk further to within your organization's risk management strategy by focusing on activities that require using highly sensitive data for information sharing, analytics and business intelligence use cases that were previously inaccessible.
- Experiment with prioritized PEC techniques in a controlled environment by establishing a working group to test the applicability and expected assurance levels that are achievable.
- Operationalize long-term protection by acquiring and/or building the tested approaches. Ensure to continue adjusting controls in response to environment risk changes, such as synthetic data diversity, the differential privacy budget and other reidentification prevention controls.

Strategic Planning Assumptions

By 2025, 60% of large organizations will use one or more privacy-enhancing computation techniques in analytics, business intelligence or cloud computing.

By year-end 2023, 75% of the world's population will have its personal data covered under modern privacy regulations.

What You Need to Know

This research is part of Gartner's Top Strategic Technology Trends for 2022.

Download the Executive Guide to Privacy-Enhancing Computation

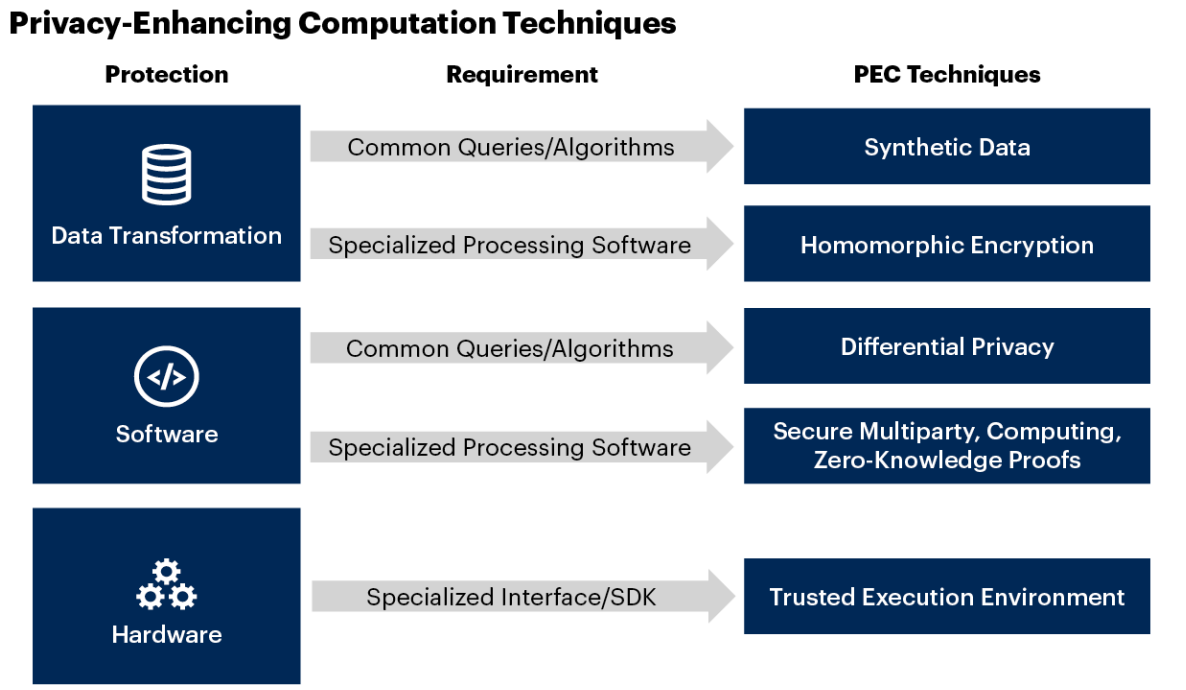
Now, more than ever, business leaders are focusing on obtaining information from data for analytics and business intelligence purposes — including data monetization and infonomics. Most often, these use cases serve secondary purposes — that is, other than the primary purpose for which the (personal) data was obtained. Such processing activities instead require anonymous data handling, following compliance risks and risks to brand, image and mainly the customer's trust. Aside from data monetization, enterprises increasingly require an exchange of information, rather than of data, for the purposes of age or identity verification, know your customer (KYC) or fraud analytics and anti-money-laundering (AML). They also often need to share or pool personal data across multiple entities. Similar confidentiality requirements may exist for nonpersonal data, like trade secrets or export-restricted information. Gartner's 2020 Board of Directors Survey shows that, amid these desired activities, regulatory/compliance risks and cybersecurity remain the top two sources of risk to the enterprise.

Meanwhile, regulatory requirements keep being added globally. Restrictions increase with regard to how personal data can be handled [1] and where it can be processed, [2,3,4,5,6] and regulatory authorities are raising the bar both with regard to the expectations of adequate security implementations [7] and even as to how AI can be used. [8,9]

PEC techniques (see Figure 1) do not provide a single answer to all of these concerns and challenges. As an umbrella for a collection of techniques, the individual use cases and challenges will determine which PEC techniques are applicable — either stand-alone or in combination with others. PEC techniques aid in the protection of privacy and confidentiality, while using data and information and, as such, ensure expanded business activities and facilitate both cross-border transfers and detailed analytics of data. PEC can also help reduce compliance and other privacy risks that currently hinder (public) cloud adoption.

Many of the individual PEC techniques are listed on Gartner's Hype Cycle for Privacy, 2021. Compared to previous iterations, we see PEC techniques move through the Hype Cycle at a reasonable pace. Secure multiparty computing (sMPC) has tipped over the peak, meaning that adoption has passed a critical point. For the first time, synthetic data indicated it will reach the plateau as expected (i.e., used by the majority of companies worldwide) in under six years — indicating a more steep adoption curve. Though individually, most PEC techniques are expected to reach the plateau from five to 10 years, as a group, Gartner expects that 60% of large organizations will use one or more PEC techniques in analytics, business intelligence or cloud computing by 2025. This is supported by evidence from Gartner's biannual Global Security and Risk Management Survey 2021, where PEC is the top investment priority for 2021 and 2022 — according to 40% of respondents (sum of the top three ranking). [10] This makes PEC a strong global strategic technology trend.

Figure 1: Privacy-Enhancing Computation Techniques



Profile: Privacy-Enhancing Computation

Description

Privacy-enhancing computation (PEC) techniques are used to identify a variety of technologies and approaches that protect data while it is used, mainly regarding confidentiality and privacy. They can be divided into three focus points:

- *Protecting the data through transformation* on the data level. Differential privacy, for example, can transform data on the fly while keeping source data intact — where synthetic data can create entire new repositories instead, and homomorphic encryption (HE) persistently transforms the source data itself.
- *Enabling the manner in which data is processed* to provide privacy protection. Federated machine learning, for example, enables decentralized usage of knowledge (i.e., of endpoint, repository or system) without transferring the actual identifiable data. SMPC — just as with HE — enables analytics of data while it remains in an encrypted state, though with specialized software.
- *Providing a trusted environment* on the hardware and hardware system level, where sensitive data can be processed or analyzed. It includes trusted third parties (TTP) and trusted execution environments (TEE). Confidential computing or use of enclaves are forms of a TEE.

Why Trending

The demand for processing data in untrusted environments (e.g., in public cloud) and performing multiparty data sharing and analytics continues to grow and has become elemental to an organization's success. Rather than a bolt-on approach, the increasing complexity of analytics engines and architectures mandates a by-design privacy capability. The pervasiveness of AI models and the necessity to train them is only the latest addition to privacy concerns.

Unlike common data-at-rest security controls, privacy-enhancing computation protects data in use, thus enabling the use cases described, while upholding privacy values. As a result, organizations can implement data processing and analytics that were previously impossible because of privacy or security concerns. Currently, the availability and maturity of accessible solutions in the market is such that privacy, security, analytics and IT leaders have started recognizing the opportunities and investigating PEC for further adoption.

Implications

In various use cases, adoption of differential privacy or synthetic data has become increasingly accessible and demonstrated a robust, noninvasive solution to many analytics, business intelligence and even to AI model training concerns. The main difference between the two is that where synthetic data is mostly a static representation of elements in a synthetic, "made-up" manner, differential privacy can deliver ad hoc information from identifiable data in a nonidentifiable manner.

The optional offering of TEE solutions in IaaS deliveries has especially grown across hyperscalers — though implementations and protection levels may vary in detail. Additionally, third-party offerings of TEEs and abstraction of one or more TEE setups are offered by various independent vendors.

Other technologies, such as homomorphic encryption and secure multiparty computation (sMPC), have transitioned from academic research projects to commercial solutions. They often require special, recoded software to enable computation on in-use protected data. Adoption is increasing and implementations have been observed in fraud analysis, intelligence operations, social media and advertising, finance, and healthcare.

Finally, the adoption of privacy-aware machine learning and of the larger area of federated ML is mainly visible in AI projects — mainly for (continued) training of AI models. In more fundamental verification use cases like KYC, zero-knowledge proofs (ZKPs) and subvariants, such as private information retrieval (PIR), are used more often.

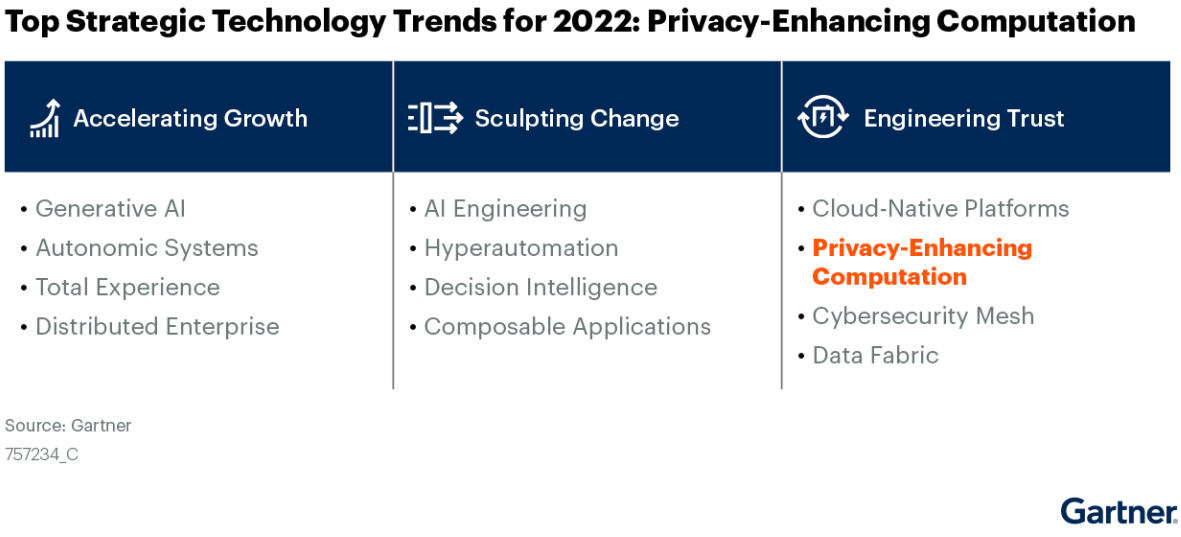
Actions

- **Identify:** Do you need to process sensitive data in untrusted environments, or use data for sharing or analytics?
- **Investigate:** Does one or more PEC technique(s) provide an adequate solution to the specific use case(s) you have identified?
- **Experiment:** Set up a working group to test the prioritized technique(s). Can you assess the adequacy of the level to which privacy protection is guaranteed?
- **Operationalize:** Purchase or build the solution(s) to implement after sufficient testing, and plan to monitor: Is the implementation robust enough?
- **Evaluate:** Does the implementation provide adequate protection over time, in line with your compliance requirements and risk appetite?

About Gartner's Top Strategic Technology Trends for 2022

This trend is one of our Top Strategic Technology Trends for 2022. The trends and technologies don't exist in isolation; they reinforce one another to accelerate growth, sculpt change and engineer trust (see Figure 2). You should explore each of these trends for their applicability to your organization.

Figure 2: Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation



Evidence

[1] State of Privacy: Since the inception and enactment of the EU's General Data Protection Regulation, many jurisdictions worldwide have developed or are finalizing new and more mature privacy legislation. Major examples include Canada, various states in the U.S., Brazil (unofficial translation of the LGPD), South Africa's work to update POPI, China, India and dozens of others worldwide.

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

The court of justice of the EU (CJEU) ruled that further restrictions should apply to international data transfers for personal data processed subject to the GDPR, as a result of which the EU-US 'privacy shield' arrangement was invalidated.

[3] Chinese Data Localization Law: Comprehensive but Ambiguous, University of Washington.

The PRC has implemented a series of laws and regulations over the past few years, and especially the Chinese Cybersecurity Act of 2018 and the upcoming personal information protection law (PIPL) put far- reaching restrictions on the ability to send data out of the country, or requirements to keep the data within the country.

[4] Data Residency – Laws and Requirements, FileCloud.

Russia, too, has enforced strict restrictions on international data transfers and data residency and has imposed various (albeit low) sanctions to major tech companies.

[5] India: Data Protection or Data Localisation, Mondaq.

The pending new privacy law in India contains similar strict requirements with regard to the need to process data in-country.

[6] Practical Privacy — Balancing Data Residency Requirements With Business Needs

[7] Recommendations, European Data Protection Board.

Various regulatory authorities up the ante on what minimum security levels to aspire or adhere to, such as the guidance on data processing after the 2020 Schrems II ruling.

[8] China "Standardises" AI Ethics, Lexology.

China AI guidance: China "standardizes" AI ethics.

[9] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts, Eur-Lex.

The EU is developing several pieces of guidance as well as regulations with regard to (personal data and) artificial intelligence within a common strategy, such as How Research and Innovation Contributes to AI Policy, European Commission; and A European Approach to Artificial Intelligence, European Commission.

For more information, see How Forthcoming EU Legal Framework Will Affect Your AI Initiatives.

[10] PRM: Gartner conducted its 2021 Annual Security and Risk survey between April and May 2019 to better understand how risk management planning, operations, budgeting and buying are performed — especially in the following areas: IT Risk management, Cybersecurity Program management, Business continuity management, Privacy and Cyber-Physical system security.

The research was conducted online among 615 respondents across NA, EMEA, APAC and LATAM regions.

Qualifying organizations have at least 100 employees and $50 million (U.S. dollar equivalent) in total annual revenue for fiscal year 2020. All industry segments qualified except for agriculture, IT services, and software and IT hardware manufacturing. Further, each of the five technology-focused sections of the questionnaire required the respondents to have certain job roles/categories and have at least some involvement or responsibility with at least one of the technology domains we explored. Interviews were conducted online, and the survey was developed collaboratively by a team of Gartner analysts — reviewed, tested and administered by Gartner's Research Data and Analytics team.

Disclaimer: Results of this study do not represent "Global" findings or the market as a whole but are a simple average of results for the targeted countries, industries and company size segments covered in this survey.

Document Revision History

Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation - 12 January 2021

Recommended by the Authors

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

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Hype Cycle for Privacy, 2021

Predicts 2021: Balance Privacy Opportunity and Risk