NOKIA

Nokia evaluates privacy-preserving technologies to protect personal data and enable new telco use cases

White paper

Our world has resolved to a great extent into a data-driven reality. From financing to Industry 4.0 manufacturing and from education to telecommunications, digital data underpins what appears to be the most significant asset value of current and future societies. Protecting and preserving data privacy is not only a fundamental human right, but also an enabler for new business models and sustainable growth.

This paper aims to raise awareness globally about the potential of privacy-preserving technologies and ways that they could be applied by the telecommunications industry. It presents Nokia's vision and Nokia Bell Labs research efforts on the critical field of privacy-preserving solutions.

NOKIA

Contents

NOKIA

Executive summary

Today we are witnessing rapid developments in the collection, analysis and use of personal data worldwide.

Notwithstanding the benefits of data processing and data analytics, for example when they support prediction of climate change, spread of epidemics or side effects of medicines, these should not come at a cost for personal privacy. It is thus of utmost importance to craft the right balance between making use of advanced technologies and protecting personal data.

Nokia, as a leader in the telco industry, is firmly committed to ensuring that when personal data is collected and used as part of its research, products and solutions, it is done in a well-governed way so that this data is adequately protected.

Privacy-enhancing techniques, such as pseudonymization, randomization, hashing and others, have been and are still being implemented, but they have also shown limitations against recent data security and privacy threats.

This situation has led to the rise of new techniques known as “privacy-preserving technologies,” including, but not limited to, data synthetization, homomorphic encryption, differential privacy, federated learning and secure multiparty computation. All these technologies are actively evaluated at Nokia and Nokia Bell Labs.

The vision is that these techniques will, in time, redefine the way data is used for the benefit of consumers, enterprises and governments in the telecommunications sector, and beyond.

For example, these techniques can reshape how operators and technology providers cooperate over the data, but also how future technologies such as cloud services, 5G technologies and the Internet of Things will enable the many benefits of the Fourth Industrial Revolution, while limiting the potential harm to society, including the loss of individual privacy.

NOKIA

An overview of privacy-preserving technologies

Data Synthesis [DS]

Synthetic data is data that is artificially created, rather than being generated by actual events. The idea is that synthetic data consists of new data points and is not simply a modification of an existing data set. It is created with the help of algorithms and bears the same key characteristics and features of the source data. Thus, it can be used for a wide range of activities, including as test data for new products and tools, model validation, or in AI model training, and can achieve near-identical results while protecting individuals' data privacy.

Homomorphic Encryption [HE]

Homomorphic encryption, considered the holy grail of privacy, is a form of encryption that allows certain computations on encrypted data, generating an encrypted result, which, when decrypted, matches the result of the same operations had they been performed on the data without encryption. Data processing can thus be performed entirely within the cypher (encrypted data) domain, allowing the data processing entity to perform its function while having no visibility whatsoever of the original data or the end results and thus protecting individuals' data privacy.

Differential Privacy [DP]

Differential privacy is a solution where a carefully calibrated noise is added to the data to disclose as much information as possible from or about the original dataset, while ensuring that re-identification of single individuals, groups or entities, is not possible. Differentially private algorithms guarantee that an attacker can learn virtually nothing more about an individual than they would learn if that person's record were absent from the dataset, thus protecting individuals' data privacy.

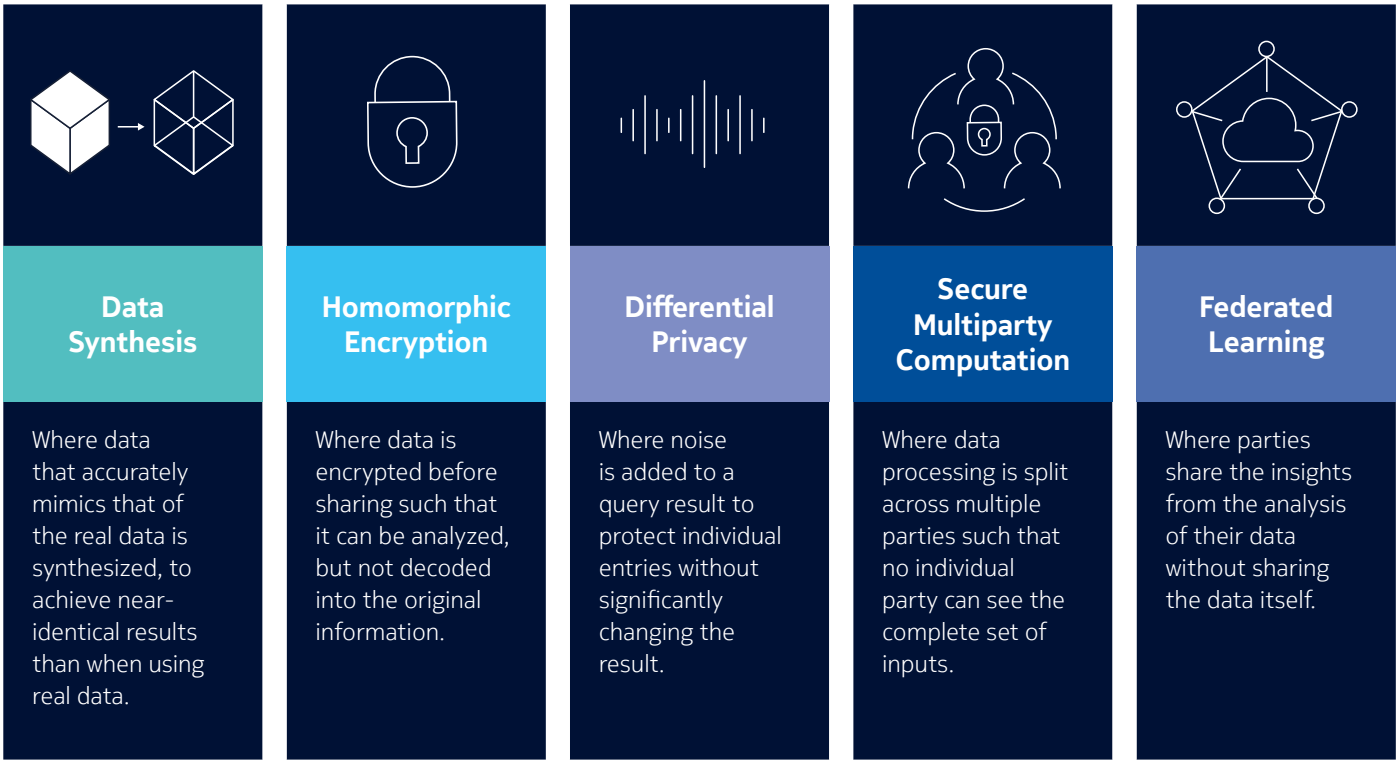
Secure Multiparty Computation [SMC]

Secure multiparty computation is a subfield of cryptography concerned with enabling private distributed computations. It allows computation and analysis on combined data without the different parties revealing their own private input. The data from input parties is securely encrypted and distributed and remains private during computation by computing parties and results are revealed to authorized result parties only, thus protecting individuals' data privacy.

Federated Learning [FL]

Federated learning is a machine learning (ML) model training approach that addresses privacy concerns by promoting the notion of learning training at the edge. Instead of collecting massive amounts of data at a centralized location and using it to train a single ML model, federated learning trains a local model with local data at each of the edge locations. This approach alleviates the need to backhaul large amounts of data for training, thus protecting individuals' data privacy.

Figure 1. Summary of privacy-preserving technologies



Supporting privacy regulation conformance around the world

The general public and the industry are becoming more aware of privacy concerns and data misuse, and as a result, societal demands and expectations of data holders or processors are higher than ever before.

New data privacy laws reflect these sentiments and make stricter regulatory demands. The EU's General Data Protection Regulation (GDPR) has led the way, inspiring similar legislation worldwide, such as the California Consumer Privacy Act (CCPA).

The use of privacy-preserving technologies can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules.

Table 1. How privacy-preserving technologies support privacy regulations' conformance

Privacy principles	How privacy-preserving technologies help with conformance
Limitation of purpose, data and storage	Support data processing & data storage minimization - [DS], [DP]
Data subject rights (right to erasure, etc.)	Support the right to erasure, e.g., the data owner can delete the raw sensitive personal data and still derive useful insights - [DS], [DP]
Privacy by design	Support privacy-by-design principles - [DS], [HE], [DP], [SMC], [FL]
Secure and limited data transfers	Support a no data transfers policy [FL], or an approach where only limited transfers are needed [DS] [DP], and secure data transfers with quantum-safe technology [HE]

NOKIA

Enabling new business models

In today's highly regulated environment, enterprises must find ways of unlocking the value of data to remain competitive. However, at present, a large part of the potential value remains untapped because of strict privacy regulations impacting how data moves through the collection, integration, processing, and dissemination stages of its life cycle.

We expect that privacy-preserving technologies will become increasingly pervasive for applications built around the privacy and security of using sensitive data, completely changing the paradigm of how organizations can leverage their data assets. The business models below represent only a small subset of the applications that privacy-preserving technologies may potentially enable in the near future.

Data innovation

Privacy-preserving technologies will facilitate use of existing sensitive or regulated data assets in legitimate ways that may previously have not been possible, because the datasets may have been too sensitive for customers or too risky. For example, mobile operators may leverage location data in new ways. The technology protections and guarantees of privacy-preserving technologies will make new high-value use cases acceptable for customers.

Data collaboration

Privacy-preserving technologies will facilitate competitive companies to see mutual benefits in sharing their data. In specific use cases, sharing data with similar companies is the best solution from an AI point of view. Indeed, you could have rival players in an industry decide that it's in their best interest to cooperate around certain mutual risks, like fraud for example. We can also envision that companies in the same industry will start sharing data and create new revenue streams thanks to privacy-preserving technologies.

Data delegation

It will become possible to delegate the execution of an ML algorithm to a computing service while retaining the confidentiality of the training and test data. This can be a major game-changer for the industry and change the cloud industry. New industry or cross-industry players may appear specializing in privacy-preserving computation and Privacy-as-a-Service (PaaS) computing business models.

Data monetization

More data marketplaces enabling companies to sell their data using privacy-preserving technologies will appear. This will help create an entirely new data industry that brings together companies who hold data with companies or individuals who need that data to innovate and create new products and services.

Figure 2. Use cases supported by privacy-preserving technologies

NOKIA

Fostering new use cases and applications

The use cases and applications below represent only a small subset of the applications of privacy-preserving technologies; however, they are the ones that Nokia believes are likely to have practical applicability and business value in the near term:

Data Retention: Storing synthetic or differentially private versions of the data without any risk to customers' privacy.

Secure Data Mining: A privacy-preserving or encrypted version of the raw data is mined.

Internal Data Sharing: Enabling sensitive data sharing internally to break down silos and foster innovation and collaboration.

Cloud Migration: Move data in the cloud without any risk to customer privacy to increase data agility.

Data Monetization: Work with partners to monetize data and create new services for consumers and new business models with partners.

Product Development: Using privacy-secured data to enable faster time-to-production, enhanced quality, and greater customer-centricity.

Vendor Validation: Provide privacy-preserving data to evaluate and select the best partners and solutions to work with.

AI/ML Model Training: Train ML models on privacy-preserved data or using privacy-preserving techniques.

Edge Computing: Train models locally, e.g., on device to remove the need to transfer customer data.

Table 2. Summary of privacy-preserving technologies enabling new use cases and applications

Use cases & applications	Data Synthesization	Homomorphic Encryption	Differential Privacy	Federated Learning	Secure Multiparty Computation
Data Retention	•		•		
Secure Data Mining	•	•	•		
Internal Data Sharing	•	•	•		
Cloud Migration	•	•	•	•	
Data Monetization	•	•	•	•	•
Product Development	•		•		
Vendor Validation	•		•		
AI/ML Model Training	•	•	•	•	•
Edge Computing				•	

Nokia's vision: Privacy-preserving solutions to create new value propositions

The world is rapidly moving toward a data-driven market economy where issues with data ownership and data sharing require the utmost focus and attention.

Access to data and data ownership are increasingly major factors in value creation and creating a system that transforms how data is collected, prioritized, and shared will create strong drivers for future value.

For the telecommunications industry in particular, having a strong governance and technological solutions to guarantee the data privacy of its customers will be a key business differentiator in the years to come.

In addition, the public and the regulators' tolerance toward privacy breaches is waning rapidly and regulatory bodies around the world are now issuing very punitive fines for failing to put proper measures in place.

As a leading actor in this global transformation, Nokia is committed to researching and enabling privacy-preserving technologies in order to propose viable production-ready solutions to its customers. Staying at the forefront of this very important technological development for the future of the telecommunications industry is crucial.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 210420 (May)