Report

The new requirements for standards for policy and mechanisms to retain privacy when analyzing users' data. information is gathered about all of us and used for a variety of reasonable commercial goals— recommendations, targeted advertising, optimizing product reliability or service delivery: the list goes on. However, the risks of leakage or misuse also grow. The two-sided market of cloud analytics emerged almost accidentally, initially from click-through associated with users' response to search results, and then adopted by many other services, whether webmail or social media. The perception of the user is a free service (storage and tools for photos, video, social media, etc.) with a high level of personalization.

There are several emerging techniques to do this that could be combined in principle, and come from the areas of hardware security and cryptography.

1) Secure enclaves
2) Homomorphic encryption
3) Multiparty Computation(MPC) 4) Edge Computing
5) Tailored approaches

Although the techniques above can be used to compute a statistical model in privacy- preserving way, namely not disclosing any unnecessary information, they do not address the problem of quantifying how much is disclosed by such a model. This (vague) question regarding "how much is disclosed" has many aspects.

Conclusion: Privacy-preserving data analysis is an emerging discipline within data science, which posts several challenges currently being simultaneously tackled from several areas such as hardware/systems security, cryptography, statistics, and machine learning. Several privacy-enhancing techniques have evolved significantly in the last decade from being mainly theoretical to becoming academic prototypes and even commercial products and, as recognized by both governments and industry, have the potential to revolutionize the field. These techniques have different tradeoffs, maturity levels, and privacy guarantees, and in some cases solve slightly different problems.