Analytics without tears

When analyzing user data, the paper discusses the requirements for standards and mechanisms for maintaining privacy. The article discusses how modern tools and techniques address these risks, from enhanced security for processing systems to controlling what results are disclosed. The current research challenges in protecting privacy fall into two categories.

Privacy-Preserving Computing: Techniques include,

* Secure Enclaves: A secure enclave's concept is based on a new technology called a Trusted Execution Environment. In such trusted hardware, encrypted private data can be uploaded, decrypted, and computed on to provide a secure virtual container.
* Homomorphic Encryption: If it is possible to perform a given operation on an encrypted data by simply manipulating its corresponding ciphertext, the encryption scheme is homomorphic with respect to that operation.
* Multiparty Computation: Several protocols exist which revolve around sharing secrets without actually disclosing them, and then computing them by transforming their shares while still keeping the secrets secret.
* Edge Computing: It stores data locally and executes analytics software on the local hubs instead of the central cloud.
* Tailored Approaches: Regression analysis and others when the problem is more defined.

Privacy Preserving Disclosure: Differential privacy is an effective way to define privacy

* DP lets us design analyses that quantify the amount of information a record gives away about whether or not it was part of the database.
* The property neutralizes linkage attacks since it is defined as a property of the analysis and not as a property of the data being analyzed.