

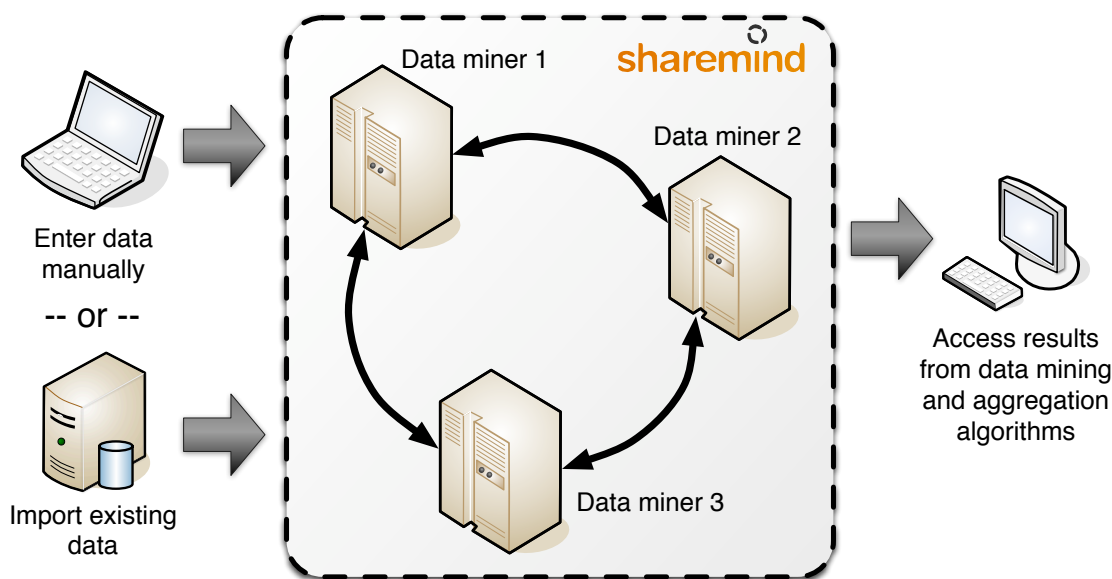
You can now **collect, store and process** sensitive data

Sharemind uses novel methods for private online data storage and processing.

- 1** Input data is divided into pieces at the client's computer and each part is sent to a separate server.

The servers can't learn secret values from the pieces
- 2** The servers exchange messages to compute new results based on the collected data.

Secret values are not leaked in the computation process.



Privacy is guaranteed during the whole analysis process

As long as the organizations hosting the servers do not exchange data, Sharemind provides perfect secrecy.

Confidentiality - only the data provider will know the secret values.

Resilience to insider attacks - even the database administrators cannot break the secrecy.

Privacy-preserving data mining - secret data can be processed to gain new knowledge.

Sharemind is unique among the competition

High performance, ease of use and strong security - all in one.

Sharemind is more efficient than other secure multi-party computation systems. It is built to work with large datasets and perform millions of secure operations in parallel. Sharemind works similarly to a database system so that developers can grasp its concepts and create applications with provable confidentiality guarantees more easily.

Turn the page for three problems that have elegant solutions with Sharemind.

Improving the security of the state

Motivation. Assume, that Homeland Security wants to gather information from telecom providers about the availability of their services in various areas of the country to make sure that in an emergency situation people have sufficient means to call for help. The system will provide alerts when the service quality is deteriorating, e.g. when multiple service providers are failing at once.

Solving the problem. The communication companies do not want to give out quality of service information as this is a business secret. However, an aggregated service report will not be a risk to any of the stakeholders and Sharemind can be used to compute these reports with significantly reduced risks.

Better marketing through collaboration

Motivation. Three friendly companies are interested in what affects the churn rates in their customer bases. Their main question is, which customers go and which ones stay. When this information is combined with the service profiles of the companies, a whole new field of customer research can be created.

Solving the problem. Sharemind can work as a shared data mining system that preserves the privacy of the individual data records provided by each company. These data records are securely aggregated so that all the companies get a report from all the shared data.

Commodity markets with bidding privacy

Motivation. Bidding markets are used to determine prices for commodities and goods. The market partners can act more honestly if they know that their bidding information is not public and it is used only in the computation for the global prices.

Solving the problem. Sharemind is ideal for systems where multiple stakeholder want to compute a common result from confidential inputs. The market will find three stakeholders with no motivation to collude who will host the computations for all the bidders.

Company profile

Cybernetica (www.cyber.ee) is an information security, information systems and navigation systems development company in Estonia. Cybernetica has developed technologies for digital signatures, timestamping, electronic voting and ID-cards. The company portfolio contains products like the Barricade2 firewall, the Privador VPN system and the SSA and ApSec security solutions.

Contact us for technical information and licensing

Contact: Dan Bogdanov (project manager) at dan.bogdanov@cyber.ee

Skype: danbogdanov

Webpage: <http://www.cyber.ee/>