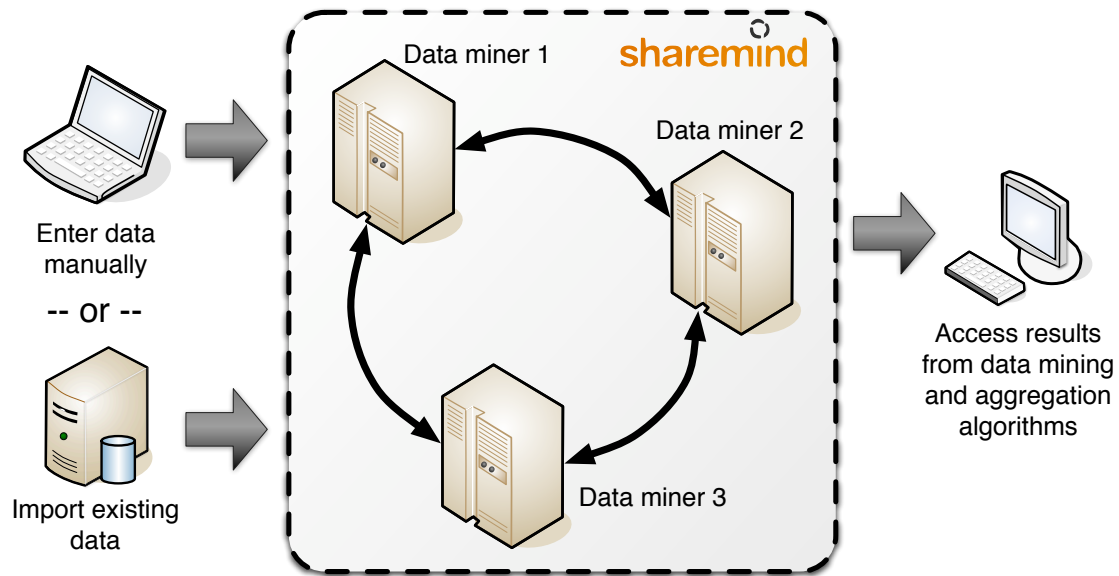


# How does the Sharemind system work?

## Deployment and development basics

The main component of Sharemind is the Miner server - a peer-to-peer application that connects to other servers in order to perform private computations. Jointly, these Miners form a distributed database with private computation capabilities. Currently, Sharemind uses three miners so three host organizations have to be elected among the stakeholders.



Note, that not every stakeholder needs to run a Miner. Other stakeholders can privately distribute their confidential data between the three Miners. Sharemind processes this data with perfect privacy, as long as none of the Miner hosts exchange their secret information with one another. This means that the users of the system need to trust the Miner hosts as a group and no unconditional trust towards any of its members is needed.

Data can be entered and results retrieved from client applications that are implemented using the Controller library. We can think of the Controller library in the same way as of a database interface - you can enter data and request computation results. The only limitation is that the Miners will refuse to disclose the contents of individual records. Instead, the Controller applications receive only the final results of the computational algorithms known to the miners. This ensures that intermediate results are not disclosed.

The algorithms in the miners are developed using the SecreC programming language - a novel programming language with built-in separation for public and private data. SecreC programs run in the hybrid execution model - private data is processed privately using secure computations whereas public data is processed normally. The algorithm preserves privacy if the private values disclosed during the execution do not leak information about the source data.

**Read on to see which features make Sharemind unique.**

# What makes the Sharemind technology unique?

These are the defining principles of Sharemind

## 1 Fundamentally better security guarantees

In any standard database system there is a system administrator who can access the data on the lower levels of the system. Standard systems need to have unencrypted data in order to process it. Sharemind uses secure multi-party computation to build a system where the power of the system administrator is of no use - the private data in the Sharemind database looks like random noise. This makes the system resilient against insider attacks.

## 2 Secure multi-party computation can be fast

Secure multi-party computation is slower than public computation because the nodes need to communicate with each other. We have built Sharemind from the ground up to be efficient also with large datasets. The Sharemind virtual machine can handle up to **100 million** parallel secure operations. Vectorization and batching allow the system to be tuned to a specific network configuration in order to achieve the best performance.

## 3 Developers need not be cryptographers

The Sharemind technology is designed to bridge the gap between secure computations and real applications. We have made our private computing system similar to a database system so that the developers and users understand its behaviour. We created developer tools and documentation to allow people with no special cryptographic skills to create applications that work with confidential data. A privacy audit is sufficient to ensure that confidential data does not leak.

### Company profile

**Cybernetica** ([www.cyber.ee](http://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](mailto:dan.bogdanov@cyber.ee)

**Skype:** danbogdanov

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