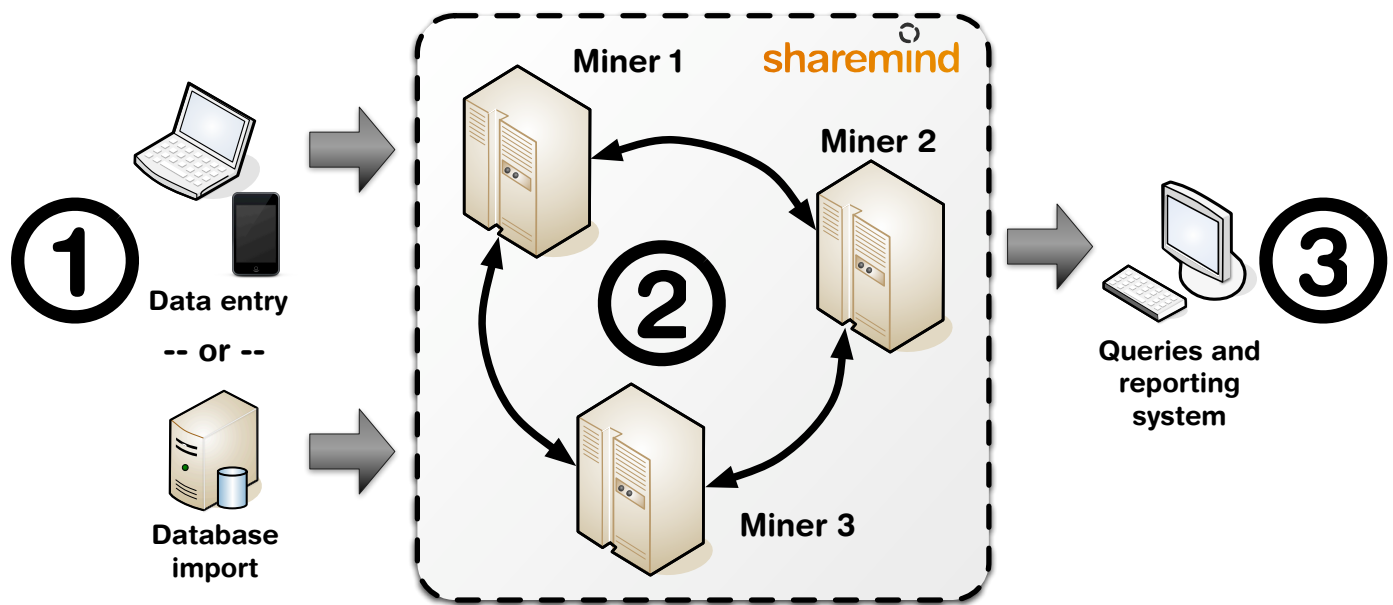


## Developing applications with Sharemind 2

How does **Sharemind** integrate with other systems?

The **data miner server** combines a secure application server with a secure database server. Three data miners are set up to satisfy the security assumptions. Sharemind servers are compatible with virtualization and can be deployed both on the cloud and by hosting providers.



- 1 Data entry and import** can be integrated into customer systems - whether mobile, web, desktop or server applications.
- 2 Data processing** algorithms for processing secure data are implemented in the **SecreC** language and loaded on data miner servers as stored procedures.
- 3 Results presentation and reporting** can also be integrated into the information system of the customer.

Read on to learn about the performance of secure computations.

# High performance secure computing

## What can **Sharemind** do?

**Sharemind** can securely store and process integer data using secure multiparty computation. Every operation is executed without any data miners learning the input or output values. The efficiency of **Sharemind** depends on the use of data parallelism in the algorithms. A single operation is less efficient than many similar operations grouped together.

Operation	Speed (1 input)	Speed (100 000 inputs)
Multiplication	87,7 op/sec	850 000 op/sec
Equality comparison	12,1 op/sec	400 000 op/sec
Greater-than comparison	9,9 op/sec	190 000 op/sec
Bit extraction	9,6 op/sec	64 000 op/sec
Division (public divisor)	7,8 op/sec	72 000 op/sec
Division (private divisor)	2,7 op/sec	9 800 op/sec

The performance benchmarks were conducted in nearly optimal conditions. Performance varies with different input sizes, network settings and server speeds.

## What are the **benefits**?

The use data parallelism and optimized protocols allow **Sharemind** to be more efficient than competing systems. The **SecreC** programming language has built-in support for optimized vector and matrix operations. The developer tools of **SecreC** are designed to reduce the time required for developing and deploying information systems using secure computations.

The efficiency and flexibility of **Sharemind** makes secure computations practical.

## 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, time stamping, 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://sharemind.cyber.ee/>