sharemind

PRIVACY ECOSYSTEM
TECHNICAL OVERVIEW

Share knowledge to learn more yourself

Process data others can't

Preserve privacy while analysing sensitive data

Sharemind™ is a database and analytics system that works on encrypted data without decrypting it

CYBERNETICA

Process private data with Sharemind™

Sharemind™ allows you to collect and analyse information that usually remains inaccessible.
Data owners who see a risk in sharing their data will find that Sharemind™ protects their assets against more threats than any other security technology.

With Sharemind's cryptographic secure computing technology, data owners share data in an encrypted form so that nobody except for themselves can access it. Even better - Sharemind™ will process the encrypted data without having to remove the encryption. Sharemind™ prevents any single party from abusing private data by distributing the control and responsibility for any operations.

Something for each privacy stakeholder

Sharemind™ helps you collect and analyse information that people usually would not give you.
Data owners who see a risk in sharing their data will find that Sharemind™ protects their assets against more threats than any other security technology.

DATA OWNERS/PROVIDERS	DATA HOSTS	DATA USERS/ANALYSTS
	DATA MANAGEMENT	
Encrypted data import and upload from databases and files. Encrypted data collection from end user web and mobile applications.	Seamless encrypted database processing and analytics - data is kept encrypted during processing. Integration with SQL/NoSQL database systems. Cloud-ready technology.	Integrations with reporting systems. Statistical analysis tools. Access analysis results from web and mobile applications or other systems.
	SECURITY	
The owner provides private data in an encrypted form. Private data is not decrypted during processing. The data holder can retain control over what can be computed. **Reduced privacy risks**	Internal and external attacks against confidentiality rendered ineffective thanks to encryption during storage and processing. Auditability of computations allows to detect tampering. **Reduced liability**	Only queries authorised by all data hosts will be processed. Compatible with differentially private analytics and other statistical privacy techniques. **Reduced liability**

The Sharemind™ privacy ecosystem

Sharemind™ is a complete solution that covers all aspects of privacy.

Encrypted Computing Core

Sharemind™ goes beyond at-rest, in transit and in-memory encryption. Sharemind™ apps keep data encrypted throughout the data lifecycle. The encrypted computing core processes encrypted values without ever having to decrypt them. All results are encrypted, until released to the client for decryption. Sharemind™ hosts can prove that they are not capable of recovering the secrets.

Machine-Enforced Privacy Policies

The encrypted computing core only releases results when allowed to do so by the privacy policy. However, Sharemind™ policies are not enforced by a single trusted party. Instead, Sharemind™ lets multiple stakeholders maintain dynamic consent that can be revoked at any time, leaving the confidential data unusable for any further processing by the other Sharemind™ hosts or clients.

Audit Support

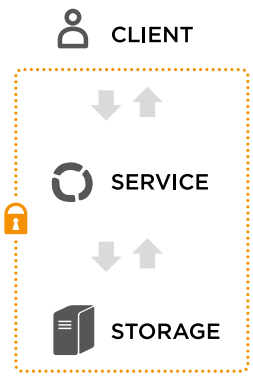
Sharemind™ keeps logs of the computing process that enable the audit of the encrypted computing core, end user activity and data use. This capability lets Sharemind™ applications ensure compliance with standards and regulations while giving unparalleled protection to the data. Both online and offline are available, depending on the kind of application.

Sharemind™ reduces the attack surface

Common application trust model

Standard application servers can encrypt data at rest (as it is kept in storage on disk or in memory) and in transit (as it is moved between services). However, the hosts of the application and database servers need to be trusted not to compromise data.

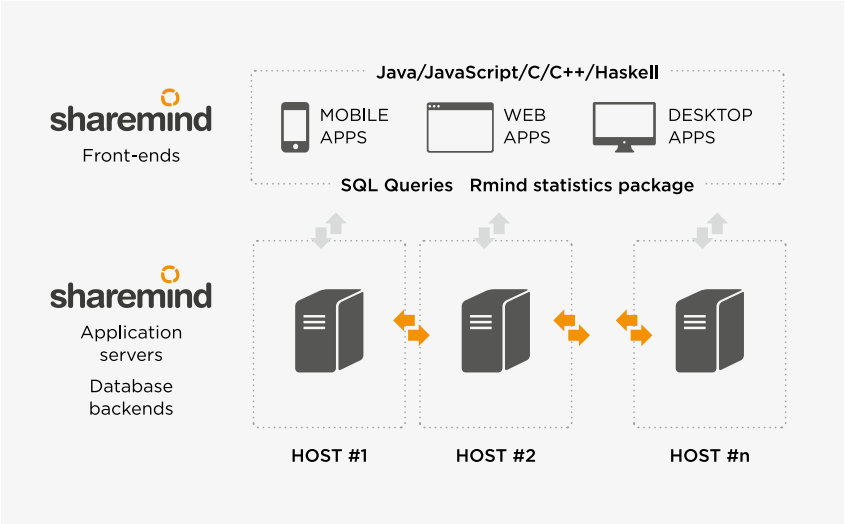
sharemind application trust model



Sharemind™ reduces the number of parties that have to be trusted. Sharemind™ makes the data owner apply encryption to the data. This encryption is not removed by the application and database servers even for processing. This way, Sharemind™ provides the completely unique encrypted-in-processing guarantee.

Sharemind™ Application Server

The Sharemind™ privacy solution is delivered within the Sharemind™ Application Server, designed according to the modern application server paradigm used by common enterprise software technologies (JavaEE, .NET etc) specifically to process data from multiple sources in a privacy-preserving way. Its distributed design avoids central control over data and Its applications have direct access to one or more Encrypted Computing Cores, Machine-enforced Privacy Policies and Audit Logging services. The applications can connect to various database backends for encrypted data storage or import of data.



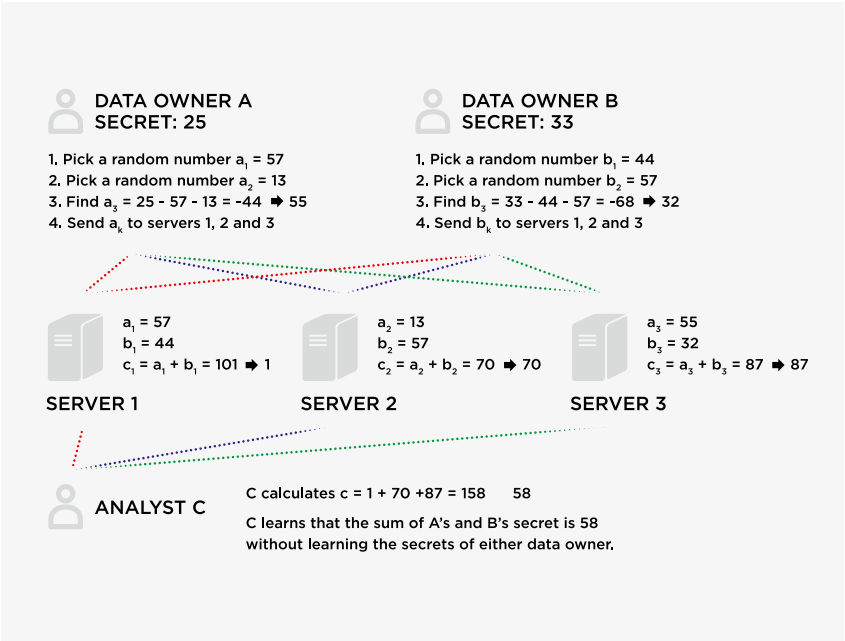
TRY THE FREE SHAREMIND™ APP DEVELOPMENT KIT

Reusable algorithms
Statistical analysis
Data mining
https://sharemind.cyber.ee

Encrypted computing? How?

The Encrypted Computing Cores of Sharemind™ take encrypted inputs and produce encrypted outputs without removing the protection. One of the efficient cores in Sharemind™ processes encrypted data shared between three servers. Its design is based on secret sharing, a cryptographic method for keyless distributed encryption. The simple example runs on two-digit numbers and shows how three servers can add two secret numbers without seeing them. All operations in the example are made on two-digit numbers. For example, (99 + 1 = 100 ➡ 0, 3 - 8 = -5 ➡ 95). Note that other operations require more complex protocols and interactions between servers. For more details on these protocols, see the Sharemind™ web page.

ENCRYPTED COMPUTING CORE



Secure operations in Sharemind™

Arithmetic / comparisons
Signed integers
Unsigned integers
Fixed point numbers
Floating point numbers
Boolean/bitwise values

Database operations
Table aggregation (group by)
Table linking (append/join)
Table sorting
Table mixing

Other operations
String processing
Ciphers/one-way functions

Sharemind™ apps have built-in policies

Sharemind™ applications are built using programming tools that have special controls for privacy. The SecreC programming language separates public and private data and forbids making private data public unless the developer explicitly asks for it using a special operator that is easy to find in code. See below for examples.

MACHINE-ENFORCED PRIVACY POLICIES

AUDIT SUPPORT

THE PROGRAMMER WRITES CODE TO...	THE ENCRYPTED COMPUTING CORE...
...declare a private value	...creates an encrypted value.
...perform an operation between two private values	...runs a secure computing protocol on encrypted inputs, getting an encrypted output
...perform an operation between a public value and a private value,	...converts the public value to a private one and uses secure computing to get the result.
...convert a public value to a private value	...encrypts the public value within Sharemind™
...convert a private value to a public one using the declassify operation,	...performs the conversion only if all Sharemind™ Application Servers agree to do this.
...publish a result to the source of the query.	...publishes the result only if all Sharemind™ Application Servers authorise the user and agree with the publication.

Each Encrypted Computing Core enforces the policy in the code. For added security, Sharemind™ Application Server hosts have to review the code before deploying it. Unless all application servers have the same code, the application cannot be run. This effectively prevents a single Sharemind™ host from forcing Sharemind™ to publish private data.

Keeping track of the work

Thanks to the end-to-end encryption Sharemind™ cannot understand the database contents that it is processing, it only knows the metadata and analysis methods. Sharemind™ can keep track of who runs queries, what data is touched and when. These logs can later be audited. The distributed nature of Sharemind™ also guarantees that there are multiple sources to help with the checking.

Lifecycle of a Sharemind™ application

Analysis

Analysts work with you to determine the data owners, their privacy expectations and the value to be extracted from the private data. You will also specify systems to integrate with, deployment models, data models and their expected volumes.

Technology

Cybernetica licenses Sharemind™ privacy technologies where needed to achieve the best privacy guarantees. For some applications, Cybernetica can provide Sharemind™ capabilities as a service.

FROM IDEA ... ... TO REALITY.

Solution design

Our security engineers will design a solution that achieves a balance between privacy and utility. We propose a combination of privacy technologies that suit with the trust model, application and the deployment model.

Development

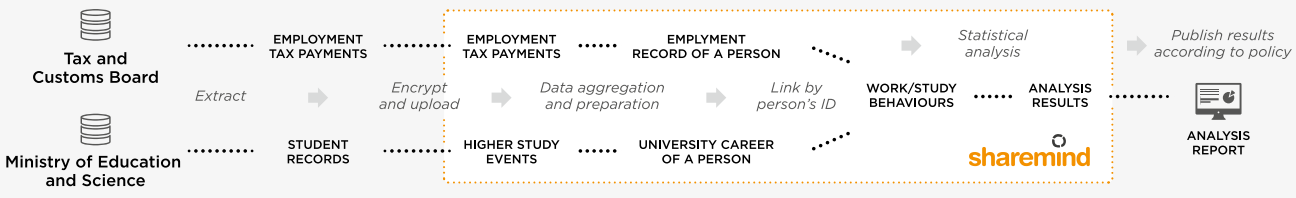
Cybernetica offers custom development services to build Sharemind™-based privacy solutions. We can also be consultants for your developers to assist in the use of privacy technologies or reaching performance goals.

CASE STUDY

Analysing private databases

Stakeholders and roles

In 2015, the Estonian Center of Applied Research used Sharemind™ to collect governmental tax and education records and run a big data study looking for correlations between working during studies and failing to graduate in time.



Results and value

The study showed that the ratios of working students is nearly equal for students in IT and non-IT curricula. However, the graduation rates of IT students were about 20% whereas non-IT students graduated with 40% success over a 6-year period. This study would not have been possible without Sharemind™, as no research organization can gain access to linked education and tax records due to Data Protection regulations. See more Privacy Stories on **https://sharemind.cyber.ee**

Strong privacy guarantees in practice

Validation

Our solutions are tested with real data or data generated by following the processes that generate data in the real world. The constructed system can be audited and reviewed with Sharemind™ tools or external parties.

Active use

Sharemind™ runs great in both single studies and analysis services. The Sharemind™ Application Server can run many simultaneous applications with multiple Encrypted Computing Cores. Each application can also have multiple users.

FROM QUALITY ... ... TO VALUE.

Deployment

Sharemind™ can be deployed in private, hybrid or public clouds with parallel architectures for increased performance. Cybernetica provides guidelines and consulting to build a proper real-world trust model.

Maintenance

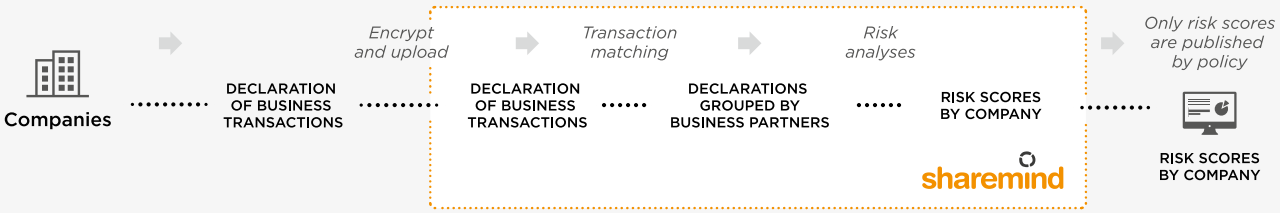
Due to privacy requirements, Cybernetica helps customers set up privacy-aware maintenance procedures. Backups, software updates and application disposal must be performed according to guidelines to ensure long-term security.

CASE STUDY

Privacy preserving fraud detection

Stakeholders and roles

In 2015, the Estonian Tax and Customs Board and Cybernetica jointly evaluated an experimental Sharemind™-based fraud detection system that collected encrypted Value Added Tax declarations from companies and analysed them to find fraud and error in tax reporting.



Goals and value

Sharemind™ makes the life of a counter-fraud agency much easier. Collection of corroborating data from other agencies or companies helps analyse and detect large-scale fraud or error and take measures to avoid it. Our experimental cloud-hosted prototype analysed a hundred million tax records within a few hours to determine key risk metrics for about 80 000 companies. The Tax and Customs Board in Estonia is considering Sharemind™ for future fraud prevention tools.

Cybernetica

OWNERSHIP
Private limited company registered in Estonia

PERSONNEL
115 employees; over 80 involved in R&D; 10% of employees with PhD

ESTABLISHED
1997 (based on structural units of the Institute of Cybernetics, 1960)

CUSTOMERS
Governmental authorities (administration, border guard, customs, maritime, police administrations, ICT-infrastructure institutions, security agencies etc); banks, telecom companies, port authorities, port crane and container spreader manufacturers, electrical installations and maintenance companies, medical institutions, railway infrastructure operators, etc

Sharemind™

Sharemind™ is the most advanced and easy to deploy cryptographically secure analytics system available.
Still, we want to be sure that your requirements and concerns are properly handled. That's why we give you a full service with security and implementation consulting. Our consulting team consists of both industry-experience solution managers and security researchers who can tackle both economic and security questions.

Contact us for more information

CYBERNETICA

CYBERNETICA AS
Mäealuse 2/1, 12618 Tallinn, Estonia
Phone: +372 6397991
E-mail: **info@cyber.ee**
Web: **www.cyber.ee**

sharemind

Sharemind™ is a registered trademark of Cybernetica AS
Web: **https://sharemind.cyber.ee**
E-mail: **sharemind@cyber.ee**
Find more privacy stories on Twitter **@sharemind**