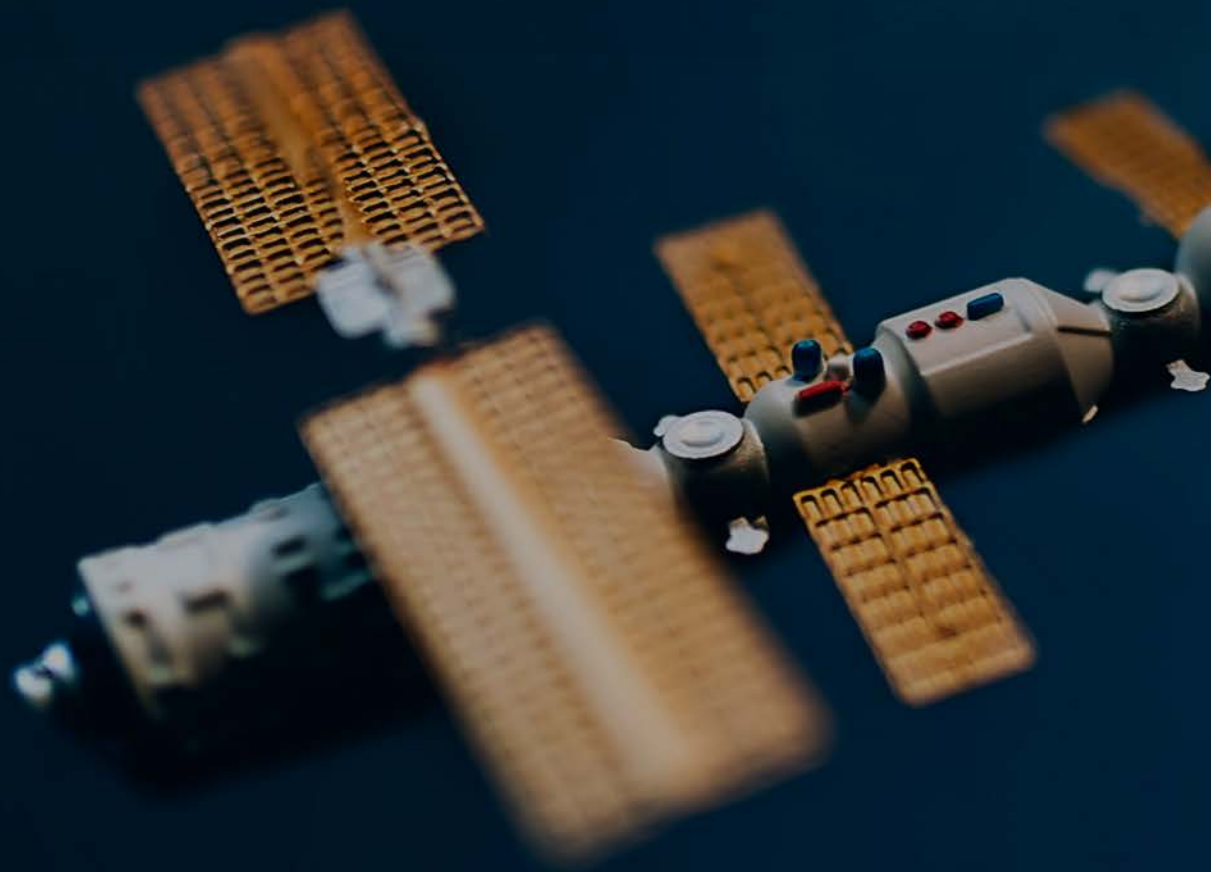


Secure computing for space safety



Cybernetica

Cybernetica is an R&D-intensive, mission-critical system development company with over 25 years of expertise. Our technologies are deployed in more than 30 countries worldwide. Our experience builds upon our capabilities to develop resilient information systems and our extensive expertise in advanced cryptography. Projects in collaboration with various institutions and governments (including the European Union, United States of America, and European Space Agency) encompass technology solutions that are highly valued by the space industry today and in the near future.



"We are extremely proud of our decades-long journey. We are certain that with our values, our people, and our capabilities, we will continue to be the driving force in emerging technologies."

– Oliver Väärtnõu, CEO

Essential facts

Established
in 1997

Roots in academia
since 1960

11% of
employees
have a PhD

Architects of
e-Estonia, incl.
i-voting, X-Road,
SplitKey

Technologies
exported to 30+
countries, incl. USA,
Japan, UAE Ukraine

Global partners
NATO, European
Commission,
DARPA, EDF,
USAFRL, ESA

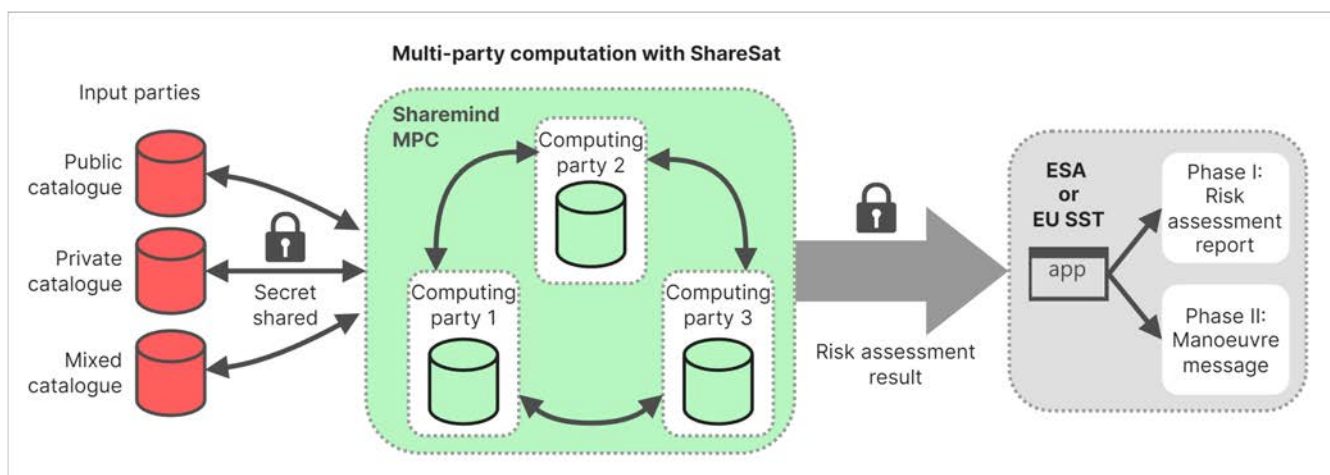
Unlocking secure space collaboration with ShareSat

How can we ensure the safety of the growing network of satellites without compromising sensitive data? The answer lies in innovative technologies like Multi-Party Computation (MPC) – the secure foundation of ShareSat project. The first multi-party computation implementation for satellite conjunction analysis was demonstrated with Sharemind in 2015.

ShareSat: transforming space data sharing

Collision avoidance software providers can integrate ShareSat's platform into their solutions. ShareSat leverages Multi-Party Computation (MPC) to address these challenges head-on. Here's a breakdown of the process:

- **Encrypted Data Input:** Each satellite operator encrypts their sensitive trajectory data before sending it to the ShareSat system. This ensures that raw data is never exposed in its entirety.
- **Secure Computation:** The encrypted data from all participating operators undergoes a secure computation process. MPC algorithms perform calculations on the encrypted data without ever decrypting it, safeguarding confidentiality throughout.
- **Confidential Result Sharing:** The results of the collision avoidance calculations are shared among the participants based predetermined policies, preserving the privacy of individual trajectories.



What is Multi-Party Computation (MPC)?

Imagine you and your friends want to figure out the average age of your group without revealing each person's exact age. With MPC, you could each encrypt your age, send secret shares of it to several trusted intermediaries (a "computing parties"), and have them do the calculations, combining the results of the calculations without ever seeing any individual ages. The result – the average age – would be shared back with everyone, but no one would know anyone else's personal information.

That is essentially what MPC does: It allows multiple parties to jointly compute a function on their private inputs without revealing those inputs to each other or to any single party controlling the computation.

We can then delve into some key aspects:

- **Encryption:** Data is always encrypted throughout the process, ensuring confidentiality.
- **Decentralization:** No single entity controls the data or the computation, fostering trust among participants.
- **Secure Protocols:** MPC relies on mathematically proven protocols to guarantee the accuracy and privacy of the results.

How does Multi-Party Computation compare to other similar methods?

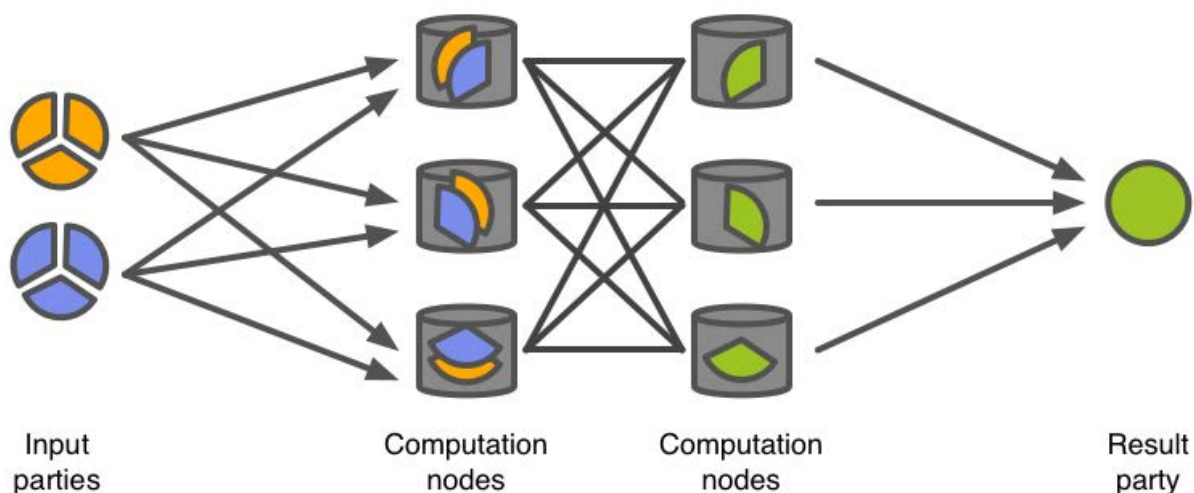
| Method | Multi-Party Computation (MPC) | Fully Homomorphic Encryption (FHE) | Differential Privacy |
|--|---|---|--|
| Data Privacy | Extremely high (data remains encrypted) | High (computations can be performed on encrypted data) | Moderate (adds noise to data while preserving aggregate trends) |
| Trust Requirements | Decentralized; no single trusted party | Requires a trusted key generator | May require a trusted party to manage noise injection |
| Computational Overhead | Can be high depending on the complexity of the computation | Very high, computationally intensive for complex calculations | Lower computational overhead than MPC or FHE |
| Suitability for Space Collision Avoidance | Excellent. Enables secure sharing of satellite trajectories without revealing sensitive details to any individual entity. | Potentially suitable, but the computational overhead might be prohibitive for real-time collision avoidance calculations. | Less ideal. While it protects individual satellite data, adding noise could affect the accuracy of collision detection and prediction. |

MPC offers a unique balance between security, efficiency, and flexibility. It allows for a wider range of computations than some other techniques while remaining relatively practical to implement in real-world applications like space exploration.

What is Sharemind MPC?

Sharemind MPC is a secure data analytics system developed by Cybernetica. It allows researchers and analysts to perform computations on sensitive datasets without directly accessing the underlying data, thus preserving individual privacy.

- **Data is Split:** Each institution splits its dataset into encrypted shares and sends them to a secure computing environment.
- **Computations are Performed on Shares:** The analysis, like calculating correlations or averages, is performed directly on these encrypted shares.
- **Results are Reconstructed:** Only the final aggregated results (e.g. the correlation coefficient) are decrypted and revealed, without ever exposing individual data points.



When do you need Multi-Party Computation?

MPC is particularly valuable when:

- **Data privacy is paramount:** Sharing sensitive information without revealing individual details is crucial (e.g., medical research, financial analysis).
- **Trust among participants is limited:** A decentralized approach mitigates the risk of a single party compromising data integrity.
- **Secure collaboration is essential:** MPC enables parties to jointly analyse data and make decisions without disclosing their private inputs.

Here are a few concrete examples across different domains:

- **Secure Financial Transactions:** Imagine you want to study the correlation between income levels and higher education dropout using datasets from different institutions like education system and tax agencies. Sharing raw data across these institutions would be a major privacy risk. Sharemind MPC comes in by enabling secure computations. [Read more](#)
- **Healthcare Data Analysis:** Researchers studying a rare disease might pool patient data from multiple hospitals for analysis to ensure individual privacy is protected. Discover how Sharemind MPC is empowering privacy-preserving genome studies. [Read more](#)
- **Secure Voting Systems:** by allowing individuals to cast their votes secretly while ensuring the integrity of the overall election results.

Collaboration opportunities during ShareSat and beyond

ShareSat builds a new era of collaboration in the space industry, enabling operators to share data securely and collectively address the challenges of an increasingly crowded orbital environment:

- **ShareSat Participation:** We are actively seeking collaborators for future projects to test ShareSat in a real-world space safety application or for projects more generally focusing on space security, data sharing, and collaborative decision-making.
- **Licensing Sharemind:** Leverage our open-source development platform, available in both TEE (Trusted Execution Environment) and MPC (Multi-Party Computation) versions, to develop secure in-house solutions tailored to your specific needs.
- **Customized Solutions:** Partner with us for the design and implementation of high-security systems incorporating Sharemind MPC, ensuring your software meets stringent privacy requirements.

ShareSat serves as a stepping stone for exploring innovative applications of Sharemind MPC in the space domain. Join us in building a more transparent, trustworthy, and innovative space ecosystem for the benefit of all stakeholders.

Cybernetica's track-record in space technologies



Minerva / European Space Agency

Project duration: 3 years 5 months

We are building a local unsupervised machine learning enabled cybersecurity toolset that will assist an IT administrator or an auditing security analyst of an SME to rapidly comprehend complex local and external network activity and to effectively identify problem areas and suspicious behaviour.

Novel methods in machine learning model visualization and entropy-based structural modelling of network behaviour will be the focus points of this technology de-risking activity.

Machine learning powered visualization of the interactions and dependencies between network hosts in a mixed-use setting, i.e. employee personal traffic, business traffic, IoT devices, cloud services, helps local IT administrator to understand effectiveness of current network defense and address found issues with host based or perimeter based mitigations.

Visualization of the interactions and dependencies between network hosts in a mixed-use setting, i.e. employee personal traffic, business traffic, IoT devices, cloud services, helps local IT administrator to understand efficiency of network defense and address found issues with host based or perimeter based mitigations.

Cybernetica's track-record in the defence domain



FAMOUS / European Commission

Project duration: 2 years 1 month

The project “European Future Highly Mobile Augmented Armoured Systems” (FAMOUS) aims at maximizing synergies, standardization and interoperability capabilities of armored vehicles to address highly demanding requirements while introducing innovative and promising new technologies and concepts. Several types of vehicles are targeted, such as future All-Terrain Vehicle (ATV), Light Armoured Vehicle (LAV) and Main Battle Tank (MBT) upgrades.



VORMSI / United States Air Force Research Laboratory

Project duration: 6 years

Estonia and United States have signed a Memorandum of Understanding to collaborate in the development of a security threat sharing and correlation system.

The project will be performed in collaboration between Cybernetica, United States Air Force Research Laboratory (USAFRL) and respective national entities that benefit from or are responsible for carrying out such information exchange. While the system will initially be used by Estonia and the United States, one of the requirements considered in the design is the capability to include additional allies in the information exchange.

The project aims to research, design and implement standards, processes, methods and rules for the exchange and processing of cybersecurity information between nations. Enabling information exchange and processing on various levels (from threats to ongoing attacks) between multiple nations with different relationships of trust and enabling different rules of information exchange dependent on the current cyber situation.

ECYSAP / European Defence Industrial Development Program

Project duration: 4 years 3 months

The main objective is to develop and implement of innovative theoretical foundations, methods and research prototypes integrated towards providing a European operational platform for enabling real-time Cyber Situational Awareness (CSA) with rapid-response defensive capabilities and decision-making support for military end-users.

An integrated and modular platform for National/European security purposes and military expeditionary operations will be developed, which shall become a realtime defensive system with cyber response capabilities, automated and deployable in areas of operations (National/European) interconnected between intelligent nodes.

The industrial consortium (Cybernetica, Leonardo, Indra, Airbus) developing the platform is being led by the Spanish company Indra Sistemas. Cybernetica participates in design, R&D activities with main focus on visualization of cyberspace and knowledge storage and management.

PROVENANCE / DARPA

Project duration: 4 years

Cybernetica was granted funding by DARPA (Defense Advanced Research Projects Agency) under PROVENANCE project to bring value to communication between the public and private sector by creating techniques for constructing meaningful zero-knowledge proofs.

The goal is to improve government interactions with citizens, companies, and other governments by enabling them to confidentially handle sensitive data. The first key objective of PROVENANCE is to build proof structures that capture real-world settings, without unreasonable simplifications. This means developing new data encoding techniques and proof structures that make the verification of proof meaningful in the real world. A further goal is to select a proof system where the deployment fits the number of stakeholders and their trust. Once the proof structure and system are known, a tool is needed to translate the statement into the underlying cryptographic constructions.

Contact our privacy technologies team for more information



Baldur Kubo
Business Development
Privacy Preserving Technologies
baldur.kubo@cyber.ee



Sandhra-Mirella Valdma
Project Manager
sandhra-mirella.valdma@cyber.ee

- cyber.ee/solutions/privacy-enhancement
- cyber.ee/research/projects/sharesat
- cyber.ee/research/projects/minerva