fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS

math eats law for breakfast

Why are fragmentiX secret sharing appliances
the best data protection solution available for you today?

… because protecting your data with science and math
always works better than GDPR or any other law or regulation!

Table of contents

Executive Summary

One of the few areas where the majority of people can agree on is that in today's cyber domain, we are all at risk of having our sensitive data stolen, encrypted or leaked. It does not make much difference whether you are a scientist, manager, politician or an ordinary citizen - all computers and mobile devices can be hacked and your data can be used against your interests.

By using what is known as SECRET SHARING - more than 40 years old mathematical equations for protecting data - it is possible to protect any type of data by simply dividing it into a series of parts. We call them fragments and store them in different owner-defined secret locations.

Only those who know where these various storage locations are, can retrieve these pieces/fragments and get the original data back in a usable form. The danger of losing a single fragment - or a small number of fragments - is mitigated by mathematics: If a thief cannot get his hands on enough fragments, there is no damage done, because there is nothing for the thief to decrypt or read.

With fragmentiX, you can now use public cloud storage in a way that is more secure and GDPR compliant than most on-premises IT environments can ever give you.

Out-of-the-box, easy to deploy, transparent and therefore invisible to end users. Each fragmentiX CLUSTER comes with 5 years mission critical support - within 4 hours at customers site.

We are in close cooperation with
AIT Austrian Institute of Technology

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Cloud, cloud storage ... back in 1979
not even Adi Shamir could know ..

WHAT IS „CLOUD“?

Good arguments for and against
the usage of public cloud storage!

PRO CLOUD	CON CLOUD
quick and inexpensive start	someone else owns the computer and has full control
easy and fast scale up	data can be leaked without you even knowing it
no investment necessary to start	no control over the admin backends
easy to implement	costs can explode in several situations
highly trained IT security experts	the respective government has easy access to all data
less or no need at all for local IT manpower	the sellers usually try to bind you to their offer
potentially inexpensive ressources	you blindly need to trust an organisation you don’t know

When it comes to the question of how to protect secrets, mankind began very early on to develop tricks and procedures to ensure - or at least hope - that a message would only reach those for whom it was intended.

In 1979, the young cryptographer Adi Shamir – during his tenure at MIT – published the paper “How to protect a secret” - so the concept of secret sharing was born 25 years before the cloud.

The hypothetic issue was to make sure that amongst 10 Physics at least five need to be present to open the document safe – no matter which five but at least five. One or up to four out of the group should not be able to steal the data.

Based on higher polynomial functions he provided the basics of what we now call Shamir’s Perfect Secret Sharing - PSS.

By using the same mathematically sound system of equations, it is possible to bring ITS – Information Theoretical Security - to the modern cloud.

Without strong encryption and technologies like secret sharing the use of cloud, technology at computers and storages owned by global IT providers, always came with the need to entrust this global corporations and the governments under which jurisdiction they act.

Since most of the global cloud actors are US or China based the jurisdiction is – seen from an e.g. European point of view - a very thin line of defense against the abuse of data processed and stored at computers owned by “someone else”.

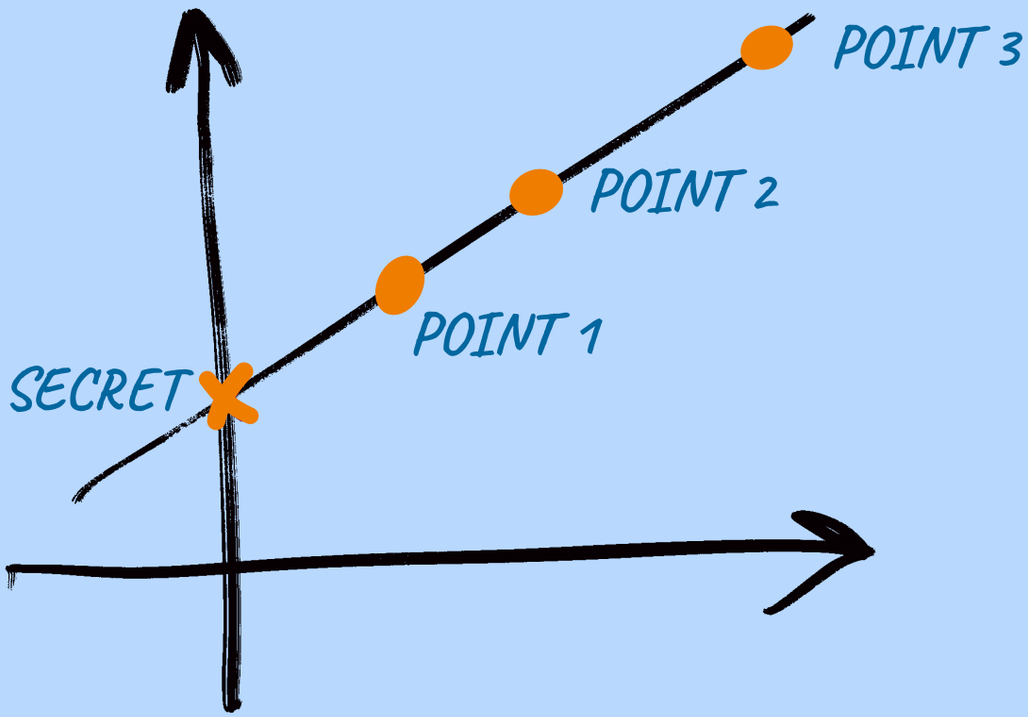
With fragmentiX secret sharing it is now possible for the first time to use the public cloud without compromising the security and the privacy of the data to be stored in the cloud. By establishing a hybrid IT environment the combined advantages of on premise and cloud computing can be used.

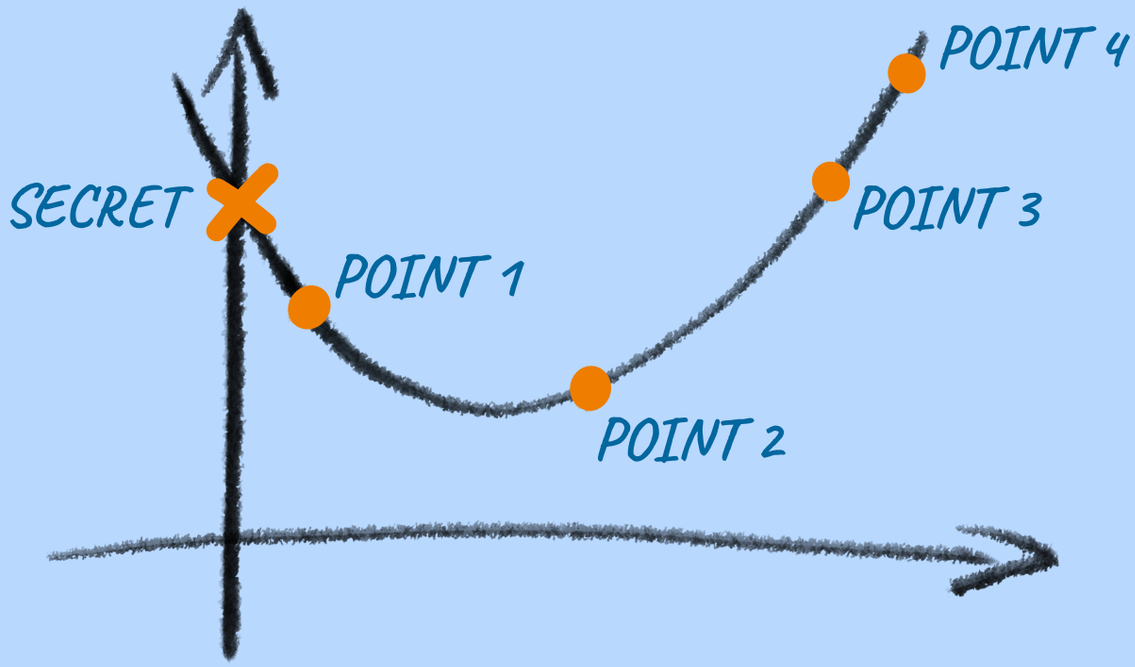
Differences & advantages compared to classic encrypted data storage in the cloud

- Although classic encryption - using a big variety of algorithms - is available since ever – only a few users actually encrypt their data before it is uploaded to cloud storages.
- To achieve ITS Informationtheoretical Security/perfect security for the „data at rest“ - the stored fragments located somewhere in the public cloud - fragmentiX makes use of OTP (OneTime Pad) and Shamir’s PSS (Perfect Secret Sharing) methods.
- This makes sure that even in the far future this cannot be cracked by any means - not even with future quantum computers.
- Also this may seem to be only theoretically relevant, the development speed of code breaking computers is enormously fast.
- With classical encryption done manually, you do not have the flexibility to define you highly protected storage scenario – whom do I need to trust?
- The necessary management of encryption keys for a single or very small group of users is manageable, but still error-prone. With fragmentiX, credentials are protected in hardware-based crypto elements that look like ordinary USB sticks.
- The upload and download of data with the https protocol takes place with classic asymmetric encryption. Security can be enhanced here by optionally using QKD - Quantum Key Distribution - to protect the data against eavesdropping during transmission.

Appliance with hardened secure operational concept/ guiderails

- IT-Security only works if provided fully automated by design.
- Can easily be integrated in an existing infrastructure
- Simply web browser based configuration with sample configurations and startup guide
- Closed hardware system - only a hardware based solution is able to provide the desired and necessary level of real secured data and operational safety.
- Separated interfaces for dedicated use, to protect against several threats coming over the cables
- Cryptographically secure high quality, self protecting smartcards to store the necessary secret credentials and configurations info.
- Secure offline configuration GUI is only accessible with “OWNER KEY” inserted.
- Updates only if initiated by owner – appliances never call home
- fragmentiX appliances are stateless: user data is only on the system while the data is processed.
- **Every fragmentiX CLUSTER appliance comes with 60 months of worldwide mission critical hardware support - within 4 hours at customers premises - executed by Dell Technologies.**





fragmentiX Secret Sharing

Imagine each of the 3 points as a fragment of your data beeing created by the fragmentiX appliance.

With a selected „frX-ratio“ of 2/3 (spoken: 2 out of 3), the line is perfectly defined with all three points and still perfectly defined if we know the position of only two points. In both cases we exactly know where the line crosses the y-axis - where our „secret“ is located.

If someone only has one fragment - or in our example only one point on our straight line - the secret could be everywhere - so a single fragment does not include any useable information.

The **„frX-ratio“** is defined as :

$$\frac{\text{the number of fragments necessary to read data}}{\text{the total number of fragments created}}$$

With fragmentiX you can create up to 26 fragments and store them in so-called LOCATIONS - buckets in S3-compatible storage that only you know about.

Since no external actor has a chance to find out where you store the fragments created from your data, this provides the highest possible protection of your data.

The same principles as for a straight line also apply to higher polynomial functions like a parabola.

A frX-ratio greater than 0.5 is recommended; e.g., 2 out of 3 or 4 out of 7.

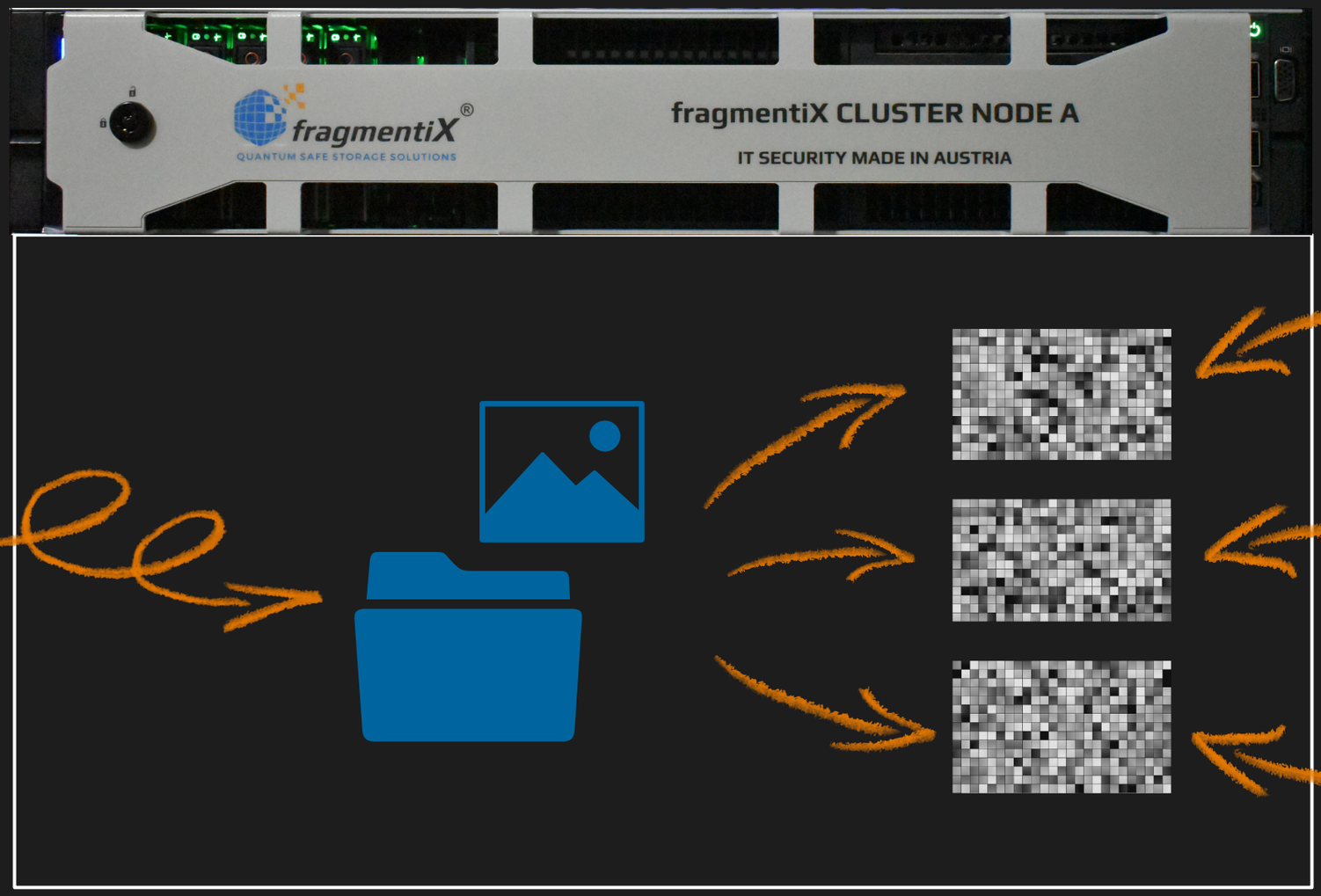
LAN side

user side

any of the availabe models of a fragmentiX appliance

WAN / Internet or VPN side

up to 26 LOCATIONS



Whether it is a single file or a large folder of a few MB, GB or TB, the fragmentiX box is agnostic and protects any type of files such as images, analysis data, project data, backups, etc. The user stores the sensitive data on a network drive previously set up by the owner/admin - and may not even know that this drive is protected by Secret Sharing.

The fragmentiX storage appliances then cryptographically splits all folders and files on this drive into a minimum of 3 and a maximum of 26 fragments. None of the fragments alone contains any usable information.

Each of these fragments is stored on a different LOCATION, which has been previously defined by the owner or administrator of the fragmentiX appliance and is also known exclusively to him.

Disaster recovery from multiple clouds

When lightning strikes, fire breaks out or floods happen, data and thus the work of entire companies is often wiped out within seconds.

Literally thousands of risks exist and locally you cannot protect yourself and your IT against too many of them.

RECOMMENDATION

Use fragmentiX to store your DR-files on 6 locations:
3 local & 3 public cloud storages with a 3 out of 6 frX-ratio and have a second fragmentiX appliance off site to start recovery from the remaining fragments to an alternative location within minutes.

Backup to multiple cloud storages

No matter what makes your data disappear, corrupted or encrypted by ransomware: a backup to the cloud looks like a good idea. However, given the risks of public cloud storage leaking or access by governments for whatever reason is a danger to all your sensitive data in backup files.

Backup files are like heaven or an all-you-can-eat buffet for data thieves and spies - everything served in single place!

RECOMMENDATION

Use fragmentiX to store your backup on 6 locations:
Use an frX-ratio of 3 out of 6 with 3 local & 3 public cloud storages.

Digital longtime archive

To ensure that your data will still be available digitally unchanged several years from now, using a cost-effective public cloud storage facility with a high level of failover and redundancy is a good idea. You won't have to worry about migrating tapes or replacing hard drives yourself. By distributing the long-term archive across a larger number of cloud storage providers, you significantly reduce the risk of data loss.

RECOMMENDATION

Use e.g. 4 to 6 of the cheapest available S3 LOCATIONS with an frX-ratio of 2 out of 6 to make sure you have your data available, even if e.g. 3 of those providers go offline.

Check the availability of your fragments regularly and restore to new providers if cheaper S3 offers become available.

Unlimited free disk space

On premise storage is fast, but usually limited in size and growth, especially if you need it quickly!

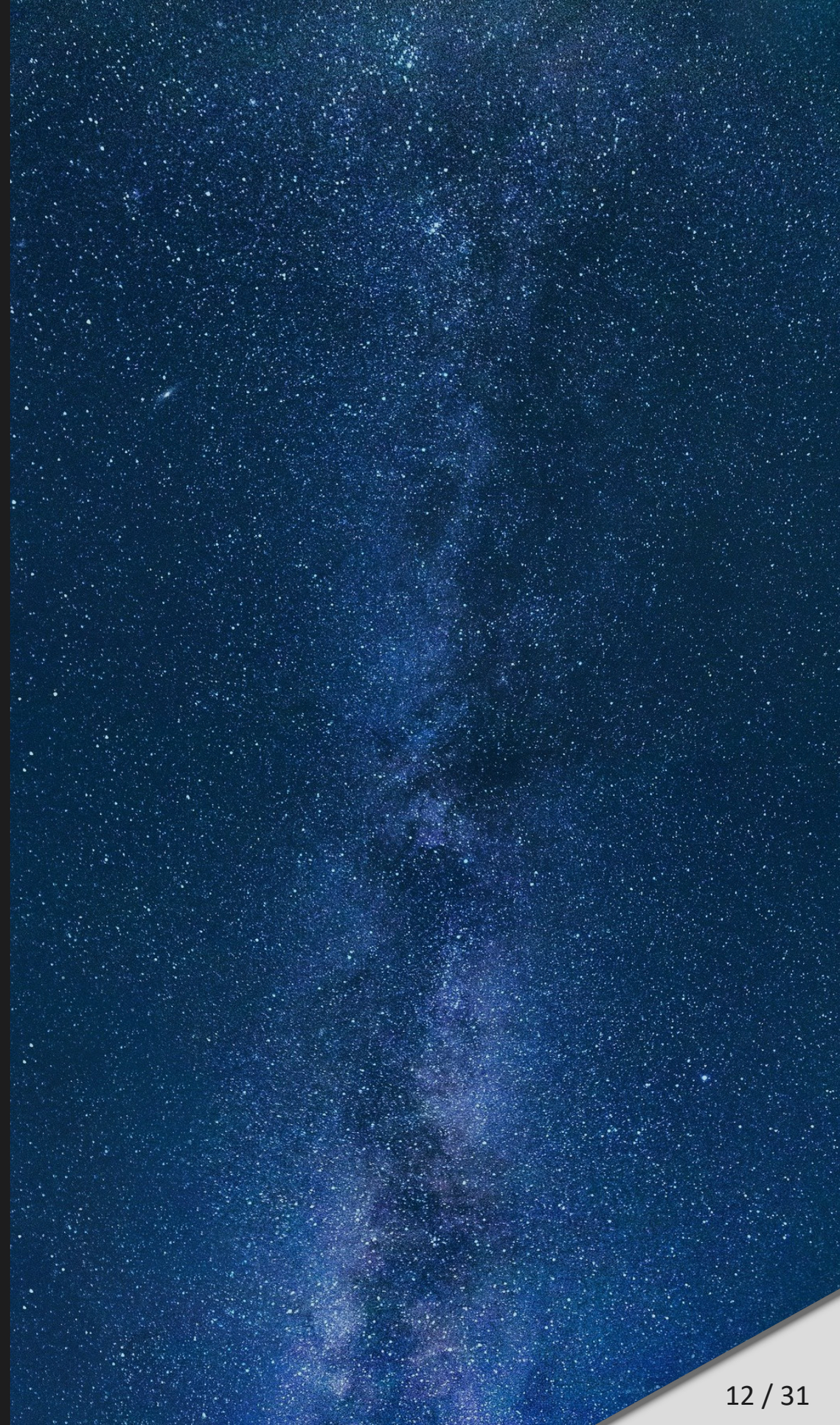
Cloud usage as a practically unlimited large hard disk is one good argument for the public cloud. To mitigate the risk or to comply with GDPR/Schrems II etc. you can use secret sharing to make sure no unauthorized party can access your data.

To share your datasets with partners using fragmentiX all of this partners need to have a fragmentiX appliance available to them.

By sharing your configuration details with your partners, you build a trusted data environment - useable by thoses authorized by you.

RECOMMENDATION

Use a 2 out of 3 frX-ratio with the best fitting latency/cost mixture you can get on the market – and check regularly for better mixtures or hybrid options (mix of local and public storages).



Temporary peak storage

In every business or research institution, there can be an unplanned need for extra storage that is not available right away and will most likely not be needed in the future.

Instead of buying local storage that might not be needed in the future – again the cloud can be a solution to make sure your external temporary storage is protected against loss, abuse and leaking, use fragmentiX.

RECOMMENDATION

Use a 2 out of 3 frX-ratio with the best fitting latency/cost mixture you can get on the market – and check regularly for better mixtures or hybrid options (mix local and public storages).

And always be aware of the hidden upload and download costs some of the best known providers will charge you!

Share research datasets and stay safe

To rightfully share sensitive data - like patient or customer records - with affiliates, the usage of mail or consumer cloud products is often neither legally nor technically acceptable.

By implementing a hybrid and federated storage system with fragmentiX, the configuration can be adapted to changing project needs and changing partners in multiple simultaneous scenarios.

Data exchange in compliance with GDPR and real longtime privacy protection is immediatly available by using a fragmentiX appliance.

RECOMMENDATION

If all the partners also have fragmentiX in use, you can select various frX-ratios with the best fitting latency / cost mixture.

fragmentiX is the center of a trusted research data environment.

Use storage together with friends/affiliates

Together with partnering organisations / trusted entities, you can decide to share the burden of backups and other storage needs by fragmenting your data to all your federated datacenters.

In a country like Austria - with 9 provinces - public entities could use fragmentiX scenarios to store backup and disaster recovery datasets in 9 LOCATIONS and make sure that no single province can get unlawfull access to an other provinces data.

RECOMMENDATION

Use a 6 out of 9 frX-ratio with the best mixture of storages available within your partnering fragmentiX storage group.

By using CSS (Computational Secret Sharing), the disk usage overhead is lower than with PSS (Perfect Secret Sharing) and still safe against quantum computers of our lifetimes.

Protect your intellectual property

To protect your patent relevant research documents, your strictly confidential contracts, your source codes or any other kind of IP against theft or espionage executed by internal or external actors, you should use secret sharing to store these sensitive documents and datasets on LOCATIONS only you know about.

RECOMMENDATION

Use an frX-ratio of 5 out of 10 with a mixture of local on-premises storage, public cloud - and if feasable local USB storage devices to have your fragments split between the persons willing and motivated to protect your IPs.

Protect sensitive data online & offline

In addition to the various scenarios for using public cloud storages safely with fragmentiX appliances, you can also use the same principles locally.

By using more than 3 LOCATIONS of hybrid or local storage, you can mitigate the need to trust a single administrator in your organization. He or she could not even abuse the data stored within the systems – which by itself takes away an unnecessary responsibility.

If there is need for your IT-teams to have full access to certain datasets at all times - you can use fragmentiX to make sure the internal threat is minimized.

RECOMMENDATION

Use an frX-ratio starting from 2 out of 3 to make sure no local admin or staff member can access (ab)useable information.

Protect your data on pure local USB based storage devices

To protect the most sensitive documents and datasets against loss, theft and espionage, you can apply PSS and CSS also with USB Hard disks or USB sticks.

You could give each of your e.g. 7 most trusted colleagues a USB stick, each containing a single fragment, produced by the appliance to be stored at their homes.

If a single person or any number of persons, lower than the minimum number defined in the frX-ratio, decides to abuse the data by selling it to the competition, no useable data is leaked.

By setting up a frX-ratio of 3 out of 7, you have a very high chance not to become compromised by single or twin cheaters. In addition, a burned down house of a single person - or a single lost USB stick - does not mean losing data.

RECOMMENDATION

Use an frX-ratio like 5 out of 10 and sizewise fitting local USB storage devices. Make sure you check regularly that all sticks/disks are still readable and available on request.

Bring datasets to the supercomputer

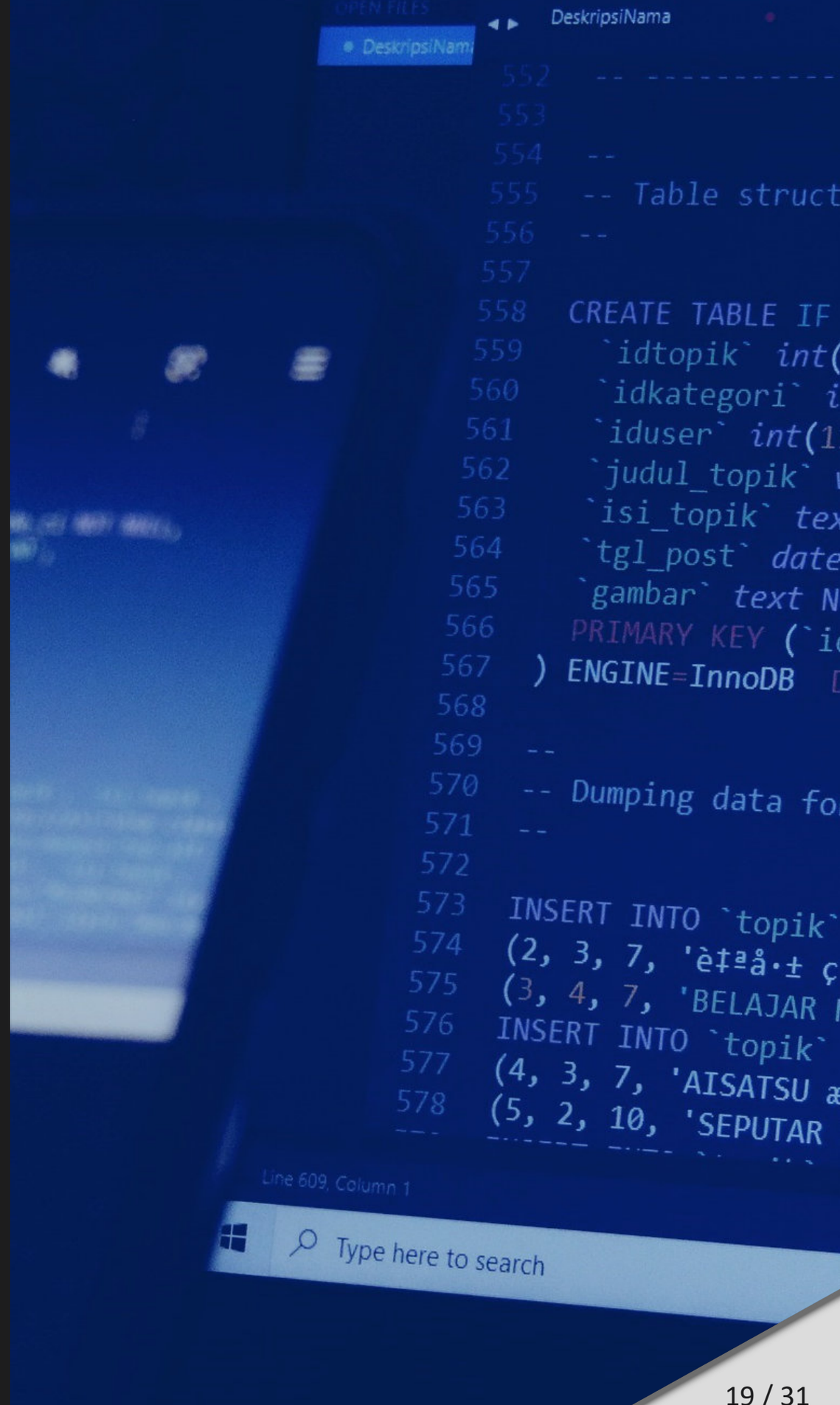
To store large datasets and programs for batch processing in a HPC/ supercomputing environment, fragmentiX provides a high performance possibility to split data to 3 or more storages before being processed and a way to deliver the results also in a highly protected storage environment.

RECOMMENDATION

Use an frX-ratio 2 out of 3 with „close to the HPC“ storages that enable you to protect your valuable data as good as possible without taking away needed throughput.

High bandwith, low latency and as short as possible waiting time in the queue.

Check out our partner Maxeler Technologies *(www.maxeler.com)*: DATAFLOW based supercomputing can save you a lot of time, money and energy!



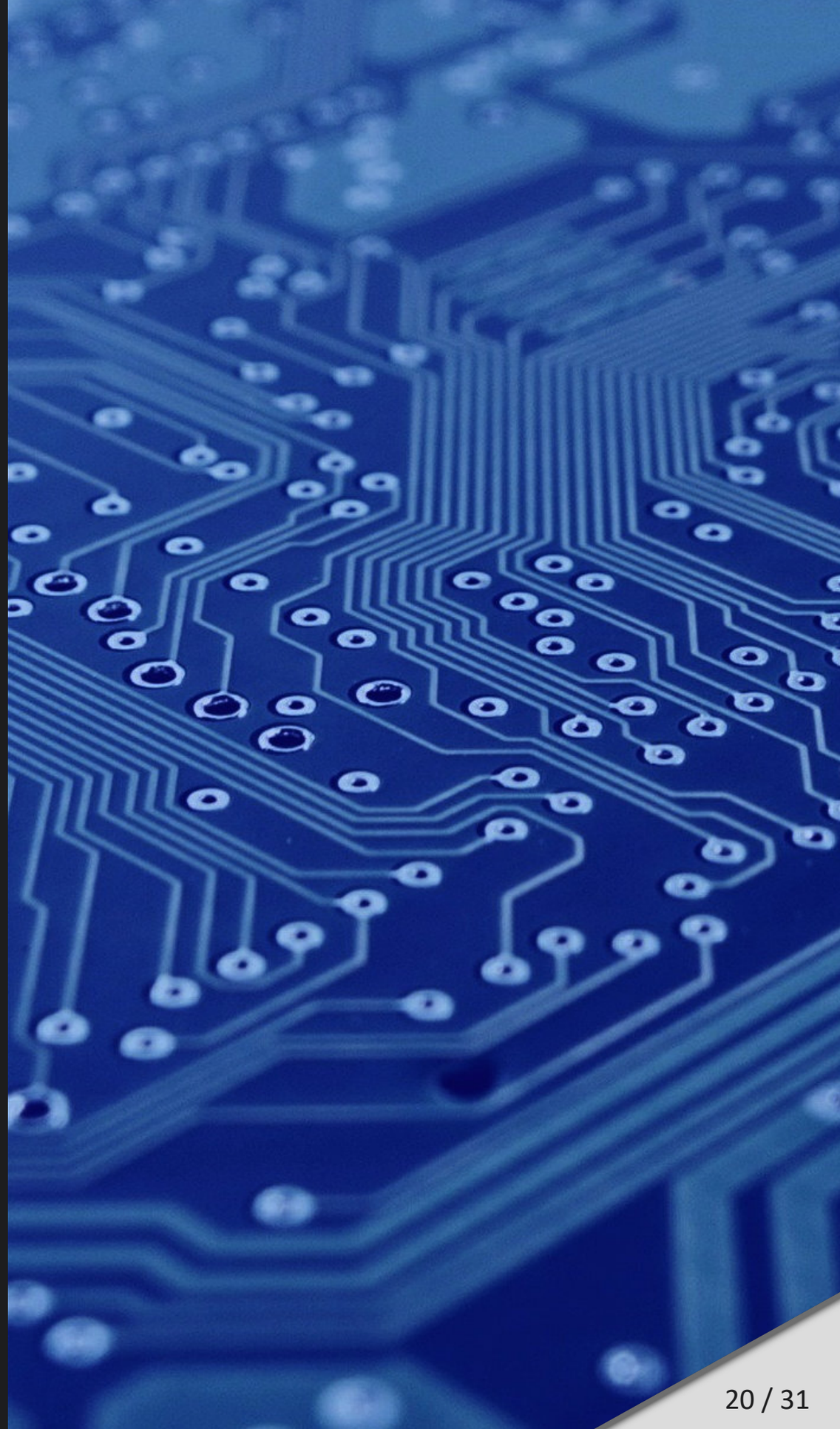
Protect your CPU against Spectre, Meltdown etc.

Together with our partner Maxeler *(www.maxeler.com)*, we offer custom circuits based protection against a lot of the known threats for industrial standard CPUs.

Since most servers and firewalls use one of these types of industrial standard CPUs, a large and publicly not very well known risk exists for all this systems.

The current generation of fragmentiX appliances is using mainstream (Intel) CPUs. With our in the near future available fragmentiX lineprotect, we can protect 4 or 8 network lines with 10 GB/s in real-time against this type of threats.

You can imagine fragmentiX/Maxeler lineprotect as a hardware based firewall protecting the firewalls and appliances on the inner side of your network.



Media archive

To store large quantities of nonpublic multimedia content in the public cloud without the risk of losing this data because of hardware problems or ransomware.

RECOMMENDATION

Use frX-ratio starting at 2 out of 3 with a mixture of local on-premise storage and cost effective public cloud storage. Because you can rely on fragmentiX for protecting the data and giving you as much as you like resilience it is possible to choose the cheaper public cloud storage suppliers.

US Cloud Act

The US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) is worth reading in detail: no matter what the big US providers will tell you: Your data is always available to thousands of US officials.

Be aware that the dominant providers will always try to argue that you are safe - and on the other side exactly those actors are not allowed by this law to let you know if they had to give your data to any of the branches of the US government.

This is not their fault - this is just a relvant law since 2018 that we all need to be aware of!

And for sure most of other geopolitical blocks care even less about e.g. European wishfull thinking about data privacy.

fragmentiX enables you to make your own choice about where on earth you decide to store your fragments.

If you want to know more about the "Five Eyes" intelligence network, you can find relevant information about it on Wikipedia, among other places.

GDPR/DSGVO

This fundamental set of privacy rules is definitly to be seen positive!

However even a good set of rules cannot protect you against thousands of actors from all places that do not care about laws and rules. To make sure only you - and those selected by you only - have access to you data - a EU law like the GDPR can not match the power of maths of secret sharing!

The big players of the internet do not have a problem paying huge fines for violating GDPR. For them it is often cheaper and easier to pay some fines than complying to rules, especially when it comes to annoying EU laws like the GDPR.

Even for best motivated organisations within the EU it is of course nevertheless difficult to comply:

- not everything is easy to understand
- for a lot of relevant issues it is difficult to find good and affordable solutions

This is where fragmentiX can solve the challange of storing and exchanging large sensitive datasets - like genome data an medical records - with the GDPR complying secret sharing technology.

No ransomware data extortion because of data-in-use encryption

To protect sensitive datasets like names, birthdates, social security numbers, banking data etc., several cryptographic principles can be applied. By using searchable encryption and storing the full data in protected vaults, you can enable your applications to only display clear text infos where necessary. In case of a ransomware attack, no abuseable data is leaked to the attacker.

RECOMMENDATION

Together with our partner Titaniam (*www.titaniamlabs.com*), we provide a broad range of protection against ransomeware and data espionage.

By integrating searchable encryption, tokenization, masking and redaction you can make sure that sensitive data is only visible in clear form where absolutly needed.

In case of a ransomware attack the risk of data extortion - you beeing blackmailed for not publishing the stolen data - can be minimized. Combined with a fragmentiX protected recovery from the public cloud you can immediatly go on working after you kicked the gangsters out of your network.

CCTV video surveillance

Most modern digital surveillance system produce huge amounts of data. Full HD, 4K and 360 degree high resolution cameras do this every single hour.

By storing CCTV footage with fragmentiX into immutable S3 buckets of several providers, you can make sure e.g. your alarm recording does not get lost or stolen by any attacker.

RECOMMENDATION

Use an frX-ratio starting at 2 out of 4 with a mixture of public cloud storage providers - and because you can rely on fragmentiX when it comes to data protection and resilience it is possible to choose the cheaper suppliers of storage in the cloud.

Because of secret sharing based privacy by design, even public entities are now enabled to use cloud storage and still comply to GDPR and other regultions.

Not any single cloud provider can see a single picture - only the owner of the fragmentiX appliance can access usable video footage.

Longtime legal evidence

In court life, the time required to store evidence can be extremely long. When a case goes to appeal, it can take even longer until data is no longer needed online.

By using fragmentiX, all parties involved in the proceedings before the court can use public cloud storages without compromizing privacy. Based on the legal system it is also possible to share evidence between two or more parties using fragmentiX as an affordable technical protection of sensitive digital evidence data.

RECOMMENDATION

Use an frX-ratio starting at 2 out of 4 with a mixture of public cloud storage - or even government on premises provided storage.

Maxeler partnership

> Protected by hard-to-penetrate custom circuits and distributed in fragments calculated via Shamir's Secret Sharing, the fragmentiX-Maxeler solution offers unprecedented data secrecy while offering scalability of multiple public cloud vendors, combined with hybrid and on-premise storage where needed.
>
> **Oskar Mencer** | *Founder & CEO Maxeler Technologies Ltd*

We are collaborating with Maxeler Technologies (Maxeler), pioneers in Maximum Performance Computing, based in London UK, to deliver maximum performance and ultra-secure-by-design data storage and computing solutions.

The products of both companies work together in several situations:

- **Maxeler's M-Space Data Platform: the collaborative research and development environment gets strongest data protection by using fragmentiX's integrated data storage architecture.**
- Maxeler's MAX5 acceleration technology: the Maximum Performance cards bring a customizable architecture to any given computational challenge and will be used in future Generations of fragmentiX products to boost performance and features available to the users.
- fragmentiX CLUSTER: the custom circuits based Maxeler technology offers additional protection for the 10GB/s WAN connections of fragmentiX CLUSTER nodes against x86 CPU related vulnerabilities like Spectre and Meltdown. The Maxeler appliance increases security on any standards-based network connection with real-time performance to mitigate all known and - as far as technically possible – still unknown vulnerabilities of major CPU technologies worldwide.

Titaniam partnership

> Addressing ransomware incidents - such as the one on JBS - involves looking at both, the mechanics as well as the economics of these attacks. When sensitive data is exfiltrated as part of the attack, victims are forced to pay out ransoms, even when they can simply restore systems from backup. We need to adopt solutions like data-in-use encryption to prevent the entire extortion cycle from being profitable in the first place.
>
> **Arti Raman** | *Founder & CEO Titaniam Inc.*

Together with Titaniam, pioneers in the field of security through data-in-use encryption, based in Silicon Valley, USA, fragmentiX can provide users worldwide with optimal protection against ransomware and other data protection threats.

The products of both companies work together in several situations:

- Titaniam's products can be implemented based on the customers specific situation - "Pre-Built" or in an "A-la-carte" way integrated into existing solutions and frameworks
- Titaniam's product SPECTRA provides a breach and extortion proof analytic store for managing sensitive data with full-featured search and analytics without decryption.
- For both ways of using Titaniam's solutions, the effect is the same: sensitive data is protected in a secured vault and only decrypted in those situations where it is absolutely necessary to have e.g. a Customer's name and address in an unencrypted version – like to print a sticker to be used for mailing.

Glossary

aws	**Amazon Web Services** the pioneers and the inventors of S3 storage, still the biggest playes worldwide
bucket	A bucket can be seen a a flat directory structure that can hold (and leak!) thousands or millions of objects (files). Buckets can be configured in often not fully undertood - ways
CCTV	**Closed Circuit Television** the old but worldwide used name for now mostly TCP/IP digital video surrveilance systems
CSS	**Computational Secret Sharing** • is the „less safe way of using secret sharing“ • uses strong symetric encryption and is still safe against future quantum computers • needs less disk space compared to PSS
FPGA	**Field Programmable Gate Array** user defineable hardware building blocks - customized for specific use - extreme performance and low power consumption
fragment	A single piece of the original file - produced using Secret Sharing mathematics. One single fragment alone never includes any useable - and therfore abusable data.
frX-ratio	Admin selectable relation between: number of fragments necessary to read files / total number of fragments produced by fragmentiX appliance (e.g. 2 out of 3)
GDPR (EN); DSGVO (DE)	**General Data Protection Regulation / Datenschutz-Grundverordnungext** EU privacy and data protection law
ITS	**Informationtheoretical Security** refers to methods such as the one-time pad that are not vulnerable to brute force attacks.
LOCATION	set of information needed to store and retrieve a single fragment - usually including a URL, a bucket name, a region and the cloud equivalent of username and password
NFS	**Network File System** very often used protocoll to share storage directories between linux/unix/host and PC systems, various versions, hogh performance
PSS	**Perfect Secret Sharing** the utmost non breakable way of encrypting data with „cryptograhic guarantee“
S3	**Simple Storage System** the amazon - and now global cloud standard for object storages with a flat structure - a so called key/value pair with metadata
SMB / samba	**Server Message Block** a protocol to connect windows and linux systems used to share directories and e.g. Printers; can be used with integrated user management

About fragmentiX

fragmentiX Storage Solutions is an Austria based IT Security company that aims at supporting individuals and companies to maintain their right for privacy and digital sovereignty.

It was founded in July 2018 by Werner Strasser who has been an entrepreneur in the fields of IT Security and digital forensics for many years. In order to foster digital sovereignty and dignity as a new to be established human right, not only for corporate and government organisations but also for individuals, he started to develop and produce quantum safe storage solutions in close cooperation with the AIT Austrian Institute of Technology.

fragmentiX products are designed for small and medium size companies as well as organizations with high performance and mission critical requirements willing to strongly protect their digital assets and knowledge against the most dangerous cloud related threats.

> We at fragmentiX are convinced that every individual human being, every company of any size as well as every state has the right to achieve Digital Sovereignty. As an Austrian and European IT company, we want to ensure that every citizen and company can effectively protect their knowledge and data against the effects of asymmetric hybrid warfare, data theft and industrial espionage.
>
> **Werner Strasser** | *Founder & CEO fragmentiX Storage Solutions GmbH*

contact us

to arrange a demonstration or talk to one of our experts!

fragmentiX Storage Solutions GmbH
IST Austria Technology Park, Plöcking 1
3400 Klosterneuburg
Austria / Europe

fragmentiX Schweiz AG
Calendariaweg 2
6405 Immensee
Switzerland / Europe

e-mail
sales@fragmentix.com

telephone
+43 2243 24203

Find one of our partners near to you on our webpage
www.fragmentix.com/partners

fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS
click here to return to TOC

The fragmentiX headquarters is located at the IST Park, the technology park of the Institute of Science and Technology Austria in Klosterneuburg, Lower Austria

IST AUSTRIA
Institute of Science and Technology

IST PARK