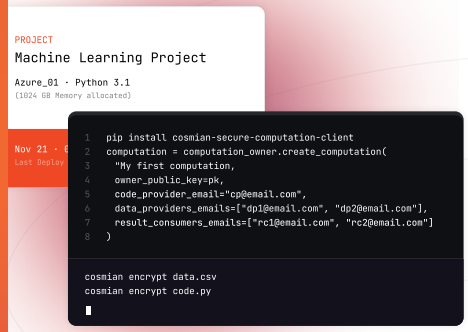
cosmian

Ubiquitous Encryption for Privacy-by-default

▸ www.cosmian.com



Data is encrypted everywhere and at all times: this is Ubiquitous Encryption

Cosmian provides libraries and server components - including in SaaS - so that developers and data engineers can easily and transparently implement privacy-by-default in applications and big data processing chains & repositories.

1. Run your models in the cloud on your clients' sensitive data while protecting your IP
2. Protect your sensitive data when in use by SaaS services
3. Harden data access of existing IT systems

Secure Computation

With Cosmian Secure Computation, data and code are encrypted with different keys and execute in a fully managed and secured environment. Only the authorized result owner can decrypt the computation results.

- ✓ Code and data encryption
- ✓ All your librairies are available
- ✓ Trigger your service when you want
- ✓ Deploy quickly using Python
- ✓ KMS included

How Secure Computation works

- Set-Up & Key Exchange
- Sending Data and Code
- Run you computation
- Receiving the Result

Cosmian Secure Computation is a serverless execution environment relying on Intel Software Guard Extensions (SGX).

Cloudproof Encryption

Cloudproof Encryption provides librairies and tools to encrypt large repositories of data - Big Data - with high performance and advanced secure techniques in zero trust environments.

- ✓ One key for each usage
- ✓ Granular control of your data access policy
- ✓ Client-side encryption
- ✓ KMS included
- ✓ Smart attributes
- ✓ Protection against cyber threats

How Cloudproof Encryption works

- Encryption
- Key distribution
- Decryption

Cosmian Cloudproof Encryption librairies are available in multiple languages facilitating encryption close to the data source and decryption close to the decryption target, including mobile devices and browsers.

Our Technology

State-of-Art encryption techniques now allow for processing calculations over sensitive data without ever accessing or exposing the data in clear text.

Secure Enclave

Isolated hardware environment where code and data are completely isolated from other applications.

Attribute-based Encryption

Public encryption schemes that gives a way to target the group of people who are authorized to decrypt.

Searchable Symmetric Encryption

Cryptographic protocol designed to securely make search queries on an untrusted cloud server.

Secure Multi-Party Computation

Set of techniques allowing several entities to jointly compute results on their inputs without revealing their individual data to others.

Functional Encryption

Enables entities to execute specific operations on encrypted data - and output the result in clear, but it will never reveal the inputs of the computation nor the intermediate values.

Fully Homomorphic Encryption

Allows to perform operations on ciphertexts without having access to the underlying source data or manipulating any secret key.

▸ Explore More at github.com/cosmian

cosmian

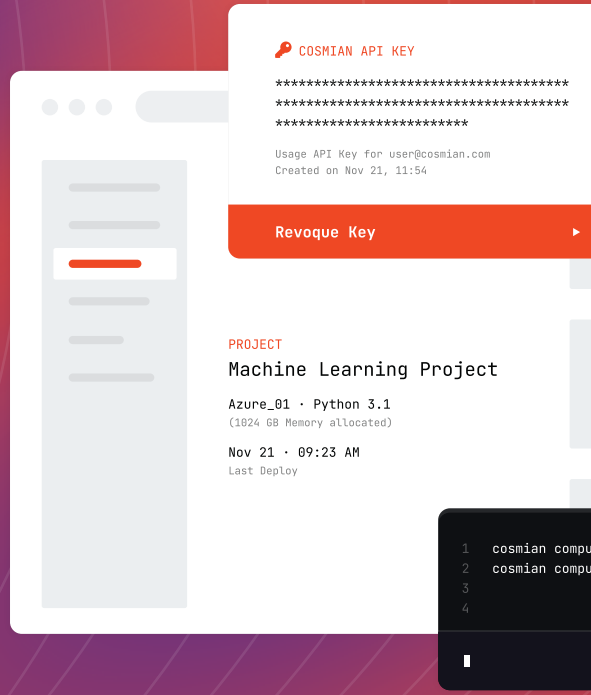
Ubiquitous Encryption for Privacy-by-default

Data encrypted everywhere and at all times for Privacy-by-default.

Secure big data repositories, decrypt sensitive data at the edge.

Encrypt confidential computations at server side.

Turn your cloud infrastructure into a zero-trust environment.



▸ www.cosmian.com