



KASPERSKY^{LAB}



SECUR'IT CUP'18

The Secure Intellectual
Surveillance



The Team



Vlad Vinogradov

Computer Vision

Deep Learning

Innopolis University



Andrey Vinogradov

Robotics

Hardware Engineering

Volga State University Of Water Transport



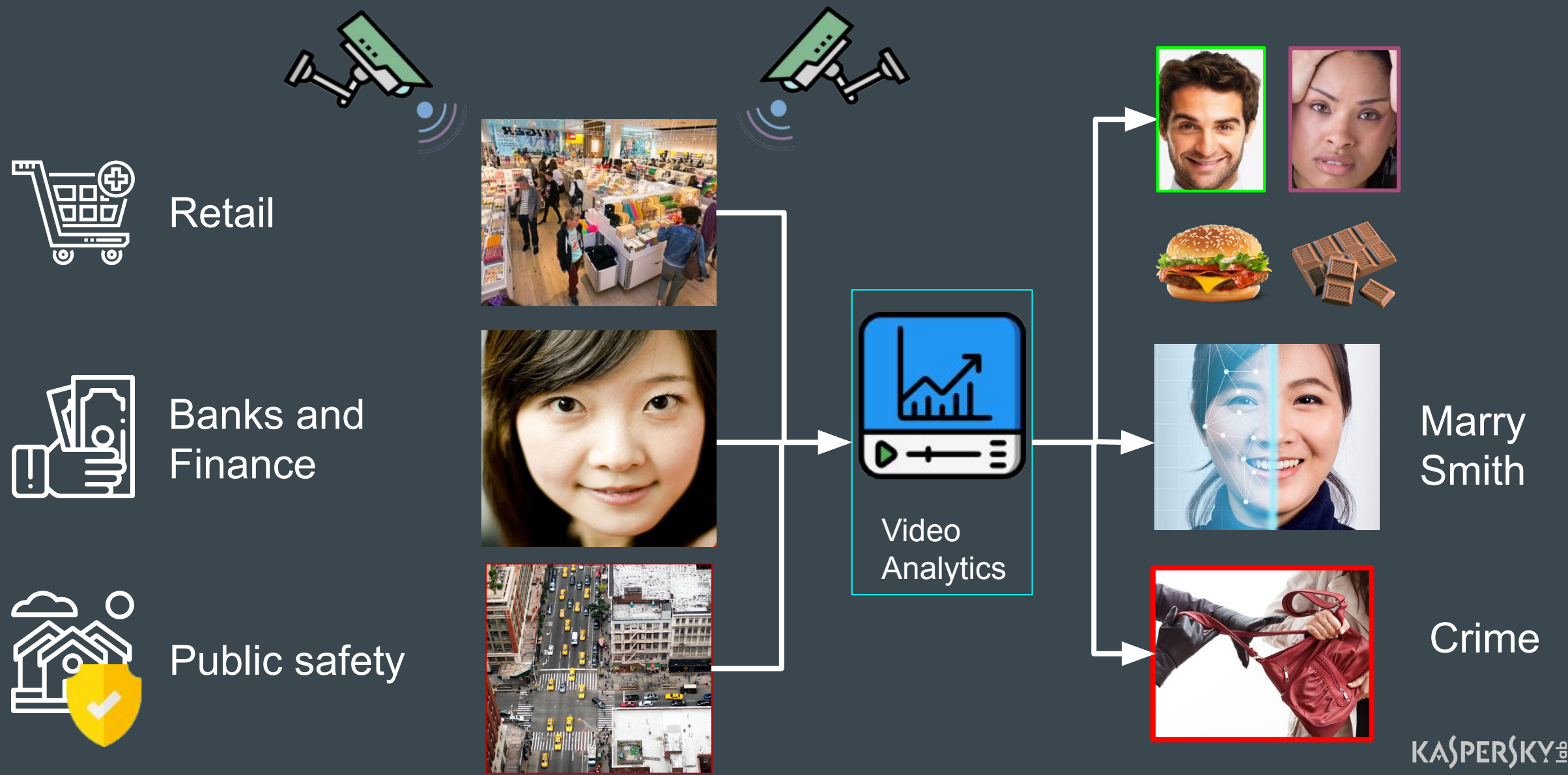
Alisa Gazizullina

Emotion Recognition

Cryptography

Innopolis University

Video Surveillance. Use cases



Limitations

Deployment problems



- Client's infrastructure: too **complex**
- Cloud infrastructure: **expensive**

Cloud Computing is Lacking Security



No encryption

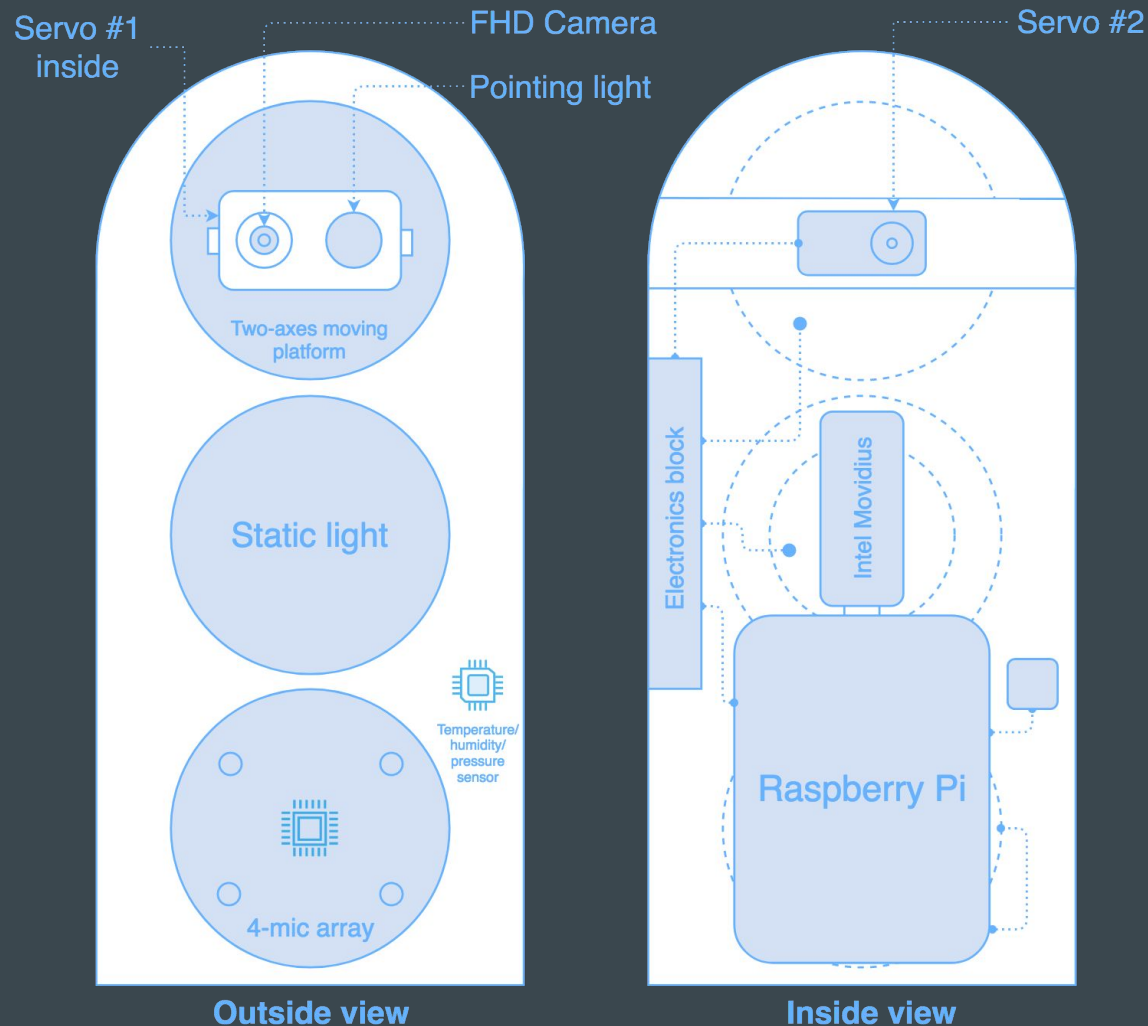
- Integrity violation
- Company's private data can be compromised



Standard Encryption

- Decryption of data at every searching operation
- Company's private data can be compromised

Solution (1/2). GPU-based camera station

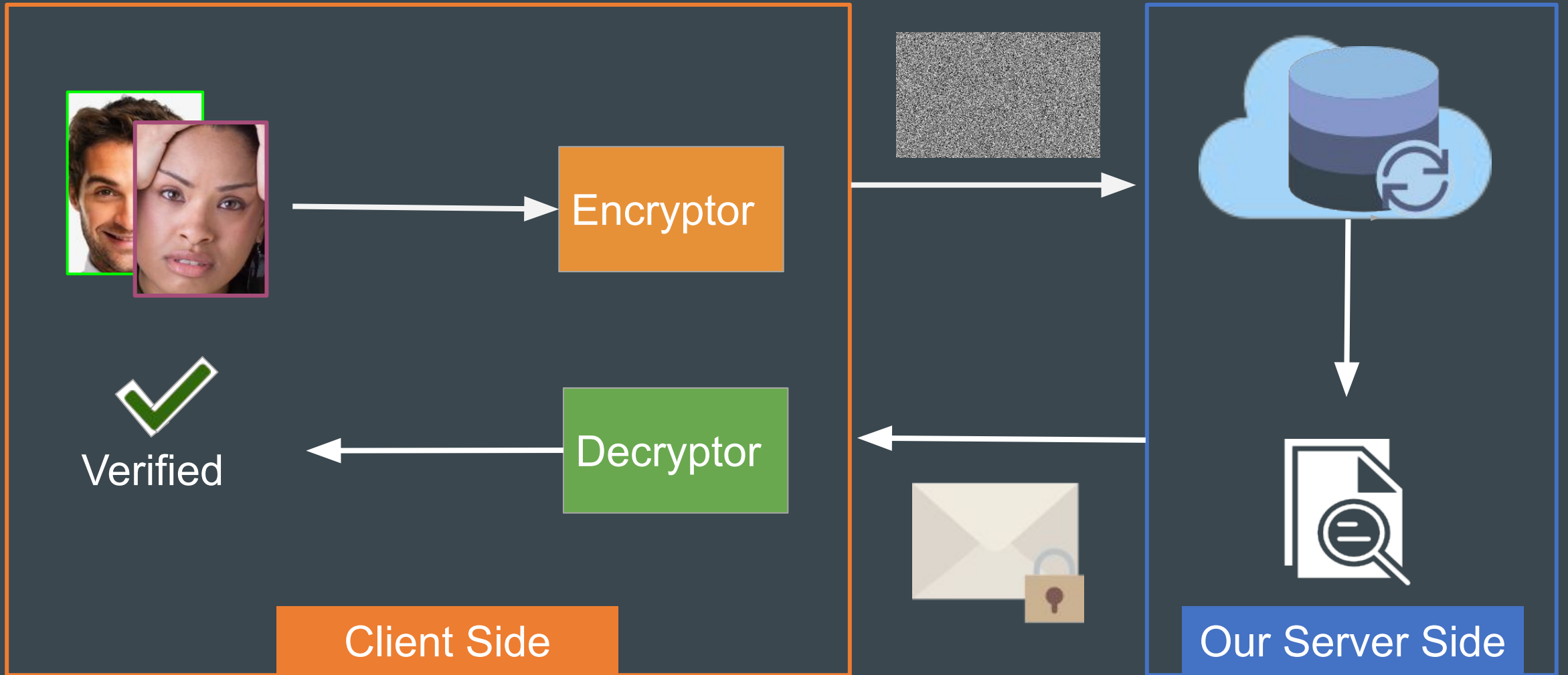


Main hardware

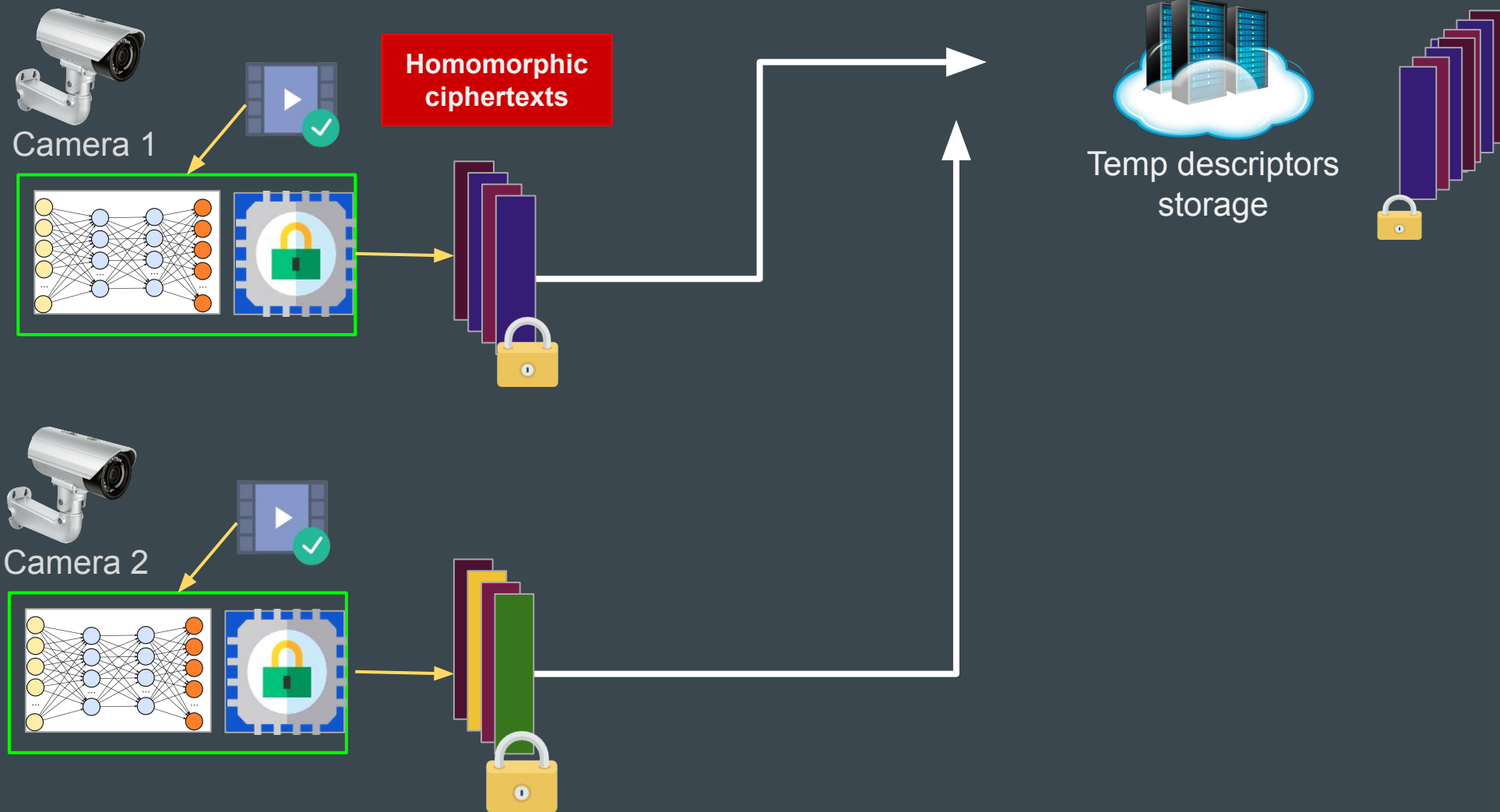
- Raspberry Pi as a platform
- Deep Learning calculations on embedded GPU Intel Movidius ®
- Full HD camera of wide angle view
- 4-mic array for sound source location

- ✓ Instant reaction
- ✓ Easy to scale
- ✓ Low network requirements

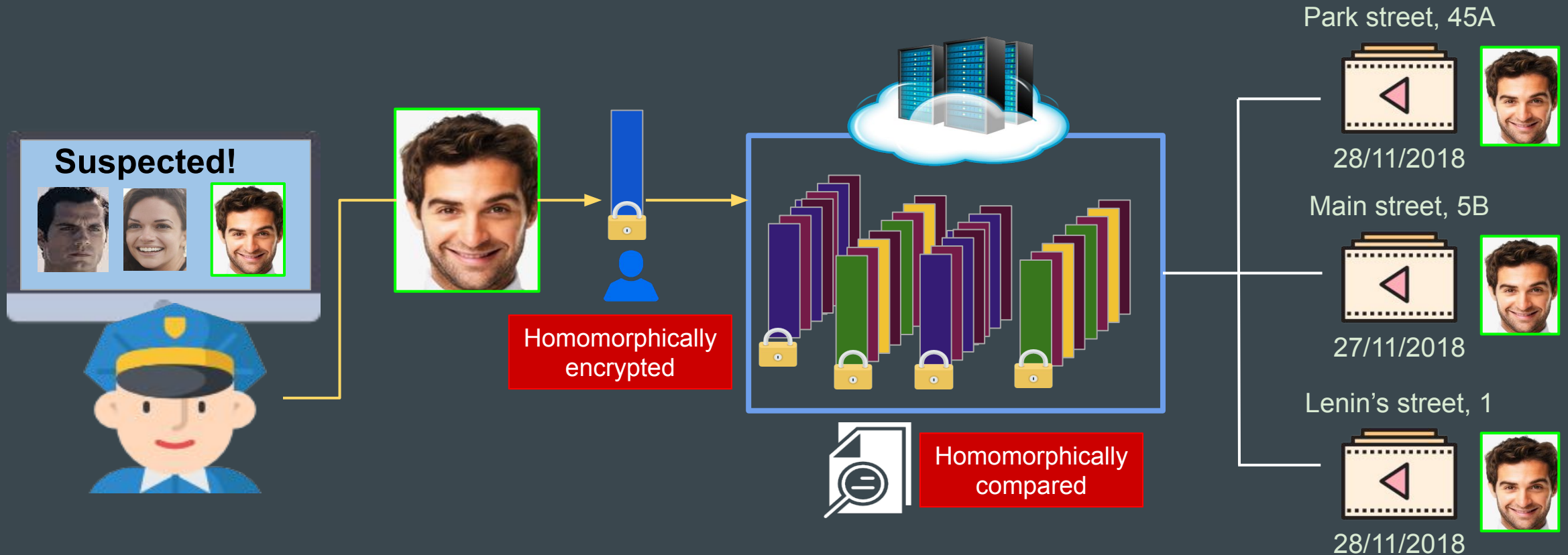
Solution (2/2). Homomorphic Encryption



Homomorphic operations (1/2).



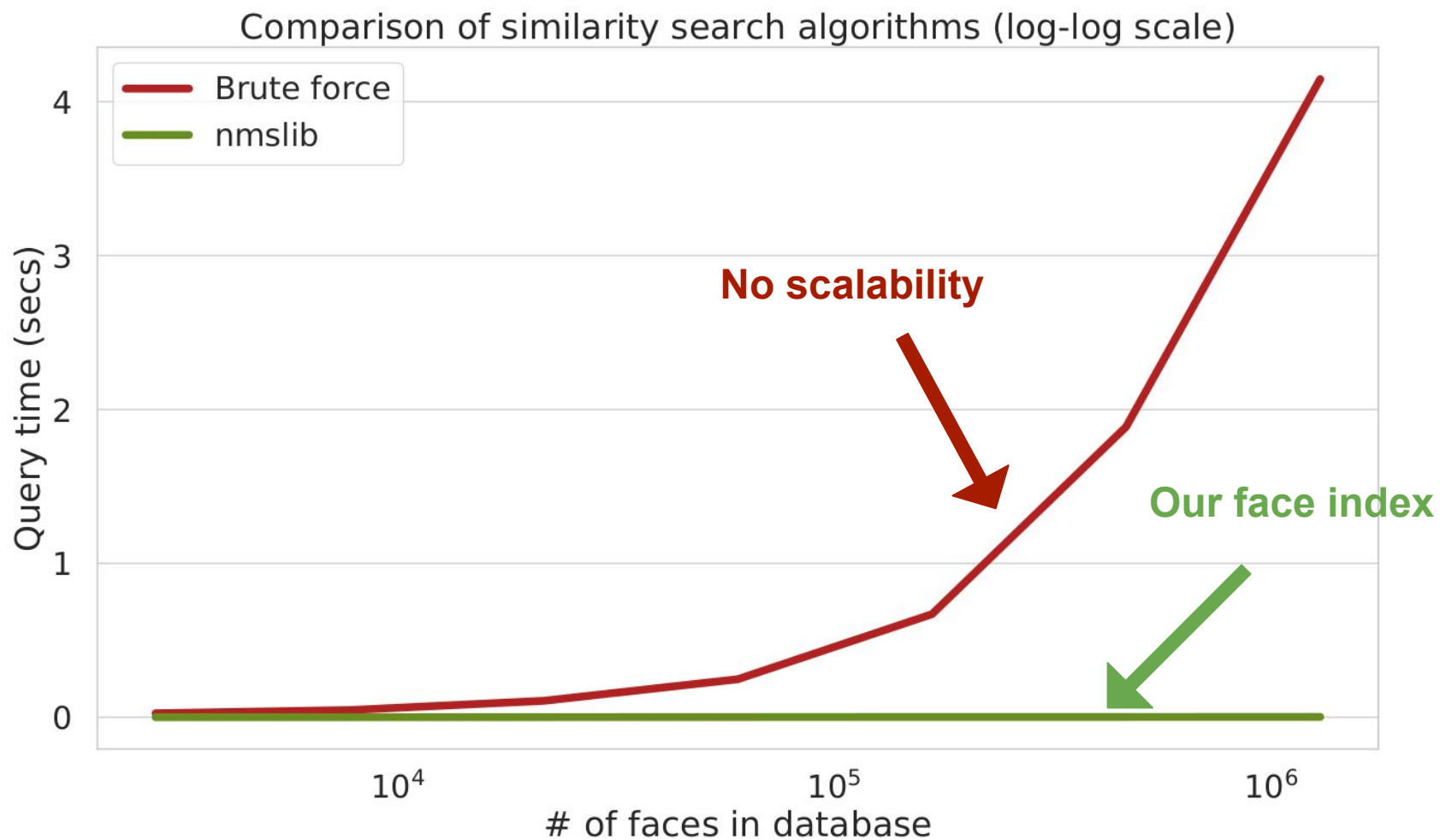
Homomorphic operations (2/2). Similarity Search



Who else?

	NtechLab	Vocord	VisionLabs	Our system
INSTANT FACE RECOGNITION	✓	✓	✓	😎
FAST LARGE-SCALE SEARCH	✓	✗	✗	😎
VIDEO MANAGEMENT SYSTEM	✓	✓	✗	😎
SECURE DATA PROCESSING	✗	✗	✗	😎
ON-DEVICE COMPUTATIONS	✗	✓	✗	😎

Scalability



**6 FPS face detection
+ recognition**

**20 msecs per query
on a million faces**

Business model

Customers
Retail
Banks and Finance
Corporate Security
Public Safety

Pilots
Ak Bars Bank
Moscow Department of Information Technologies
ChemRar - chemical factory

Easy getting started
Crime Camera Station
Subscription on REST API of video analytics service

We offer
Crime Camera Station
Face search index server (subscription)
Face control systems
People counting
Demography analysis
Face spotting on crime detection database



SECUR'IT CUP'18

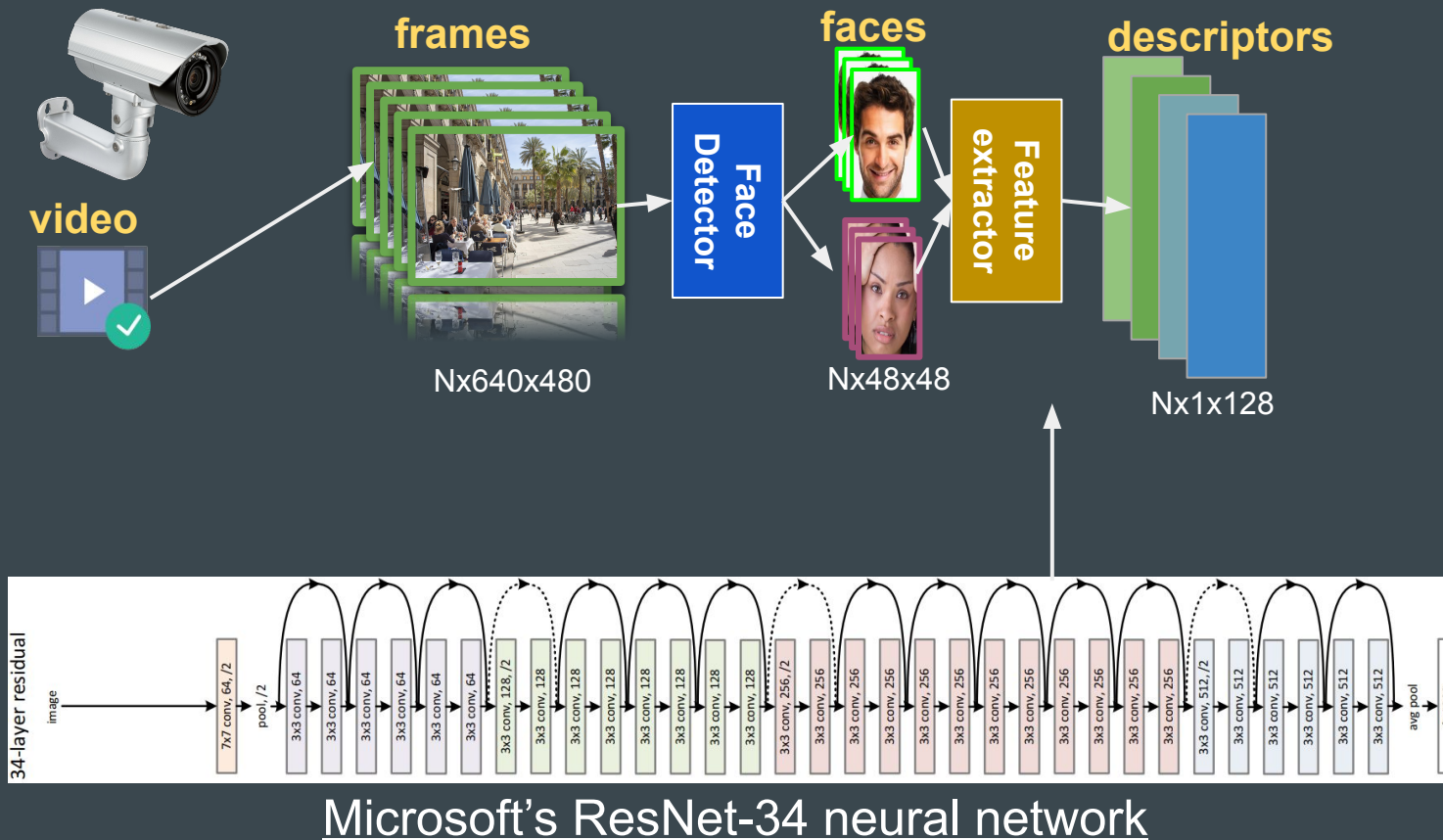
Thank you!
Questions?

Contact us:

Alisa Gazizullina: gazizullina2010@yandex.ru

Vlad Vinogradov: vladvin@eora.ru

Neural Networks for face verification



Feature extractor characteristics

Gives **similar descriptors** for the **same person**, different for others

Accuracy: **99.38%** on Labeled Faces in the Wild

Trained on **3 million** faces of celebrities (**7485 unique**)

Training was provided by Dlib library author

Libraries

Dlib.net

Machine Learning tools for real-world problems

OpenCV

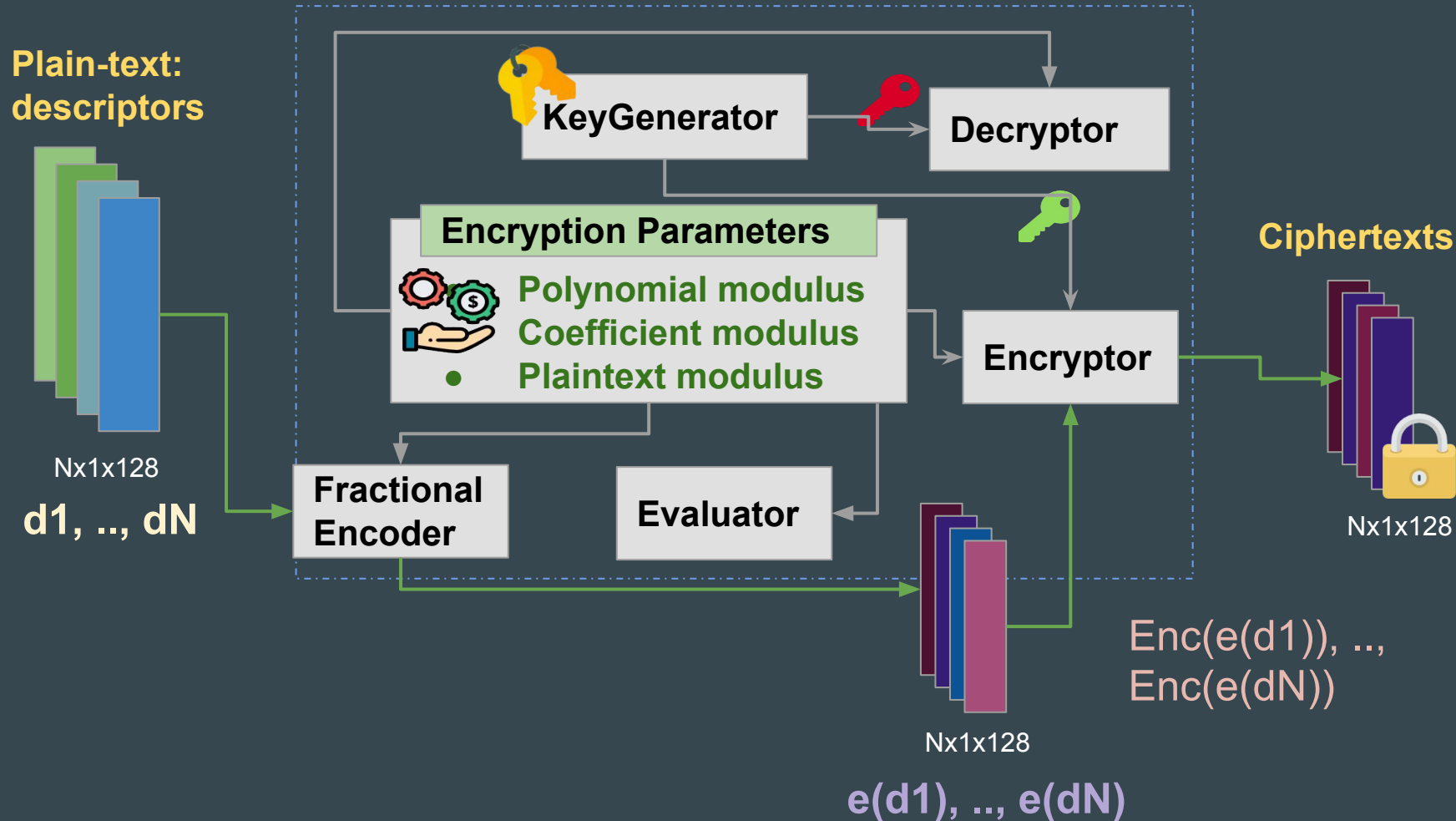
Computer Vision library

scikit-learn

Machine Learning library for science

Homomorphic Encryption Module

Homomorphic Encryption explained



Libraries

SEAL 2.3.1

Simple Encrypted Arithmetic Library
By Microsoft

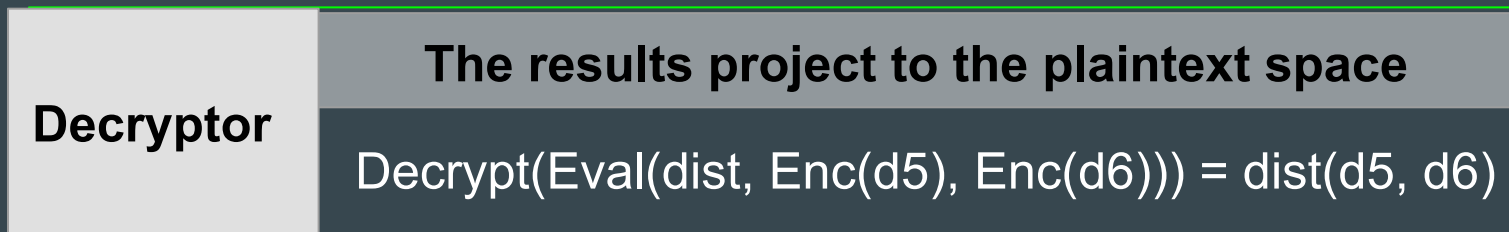
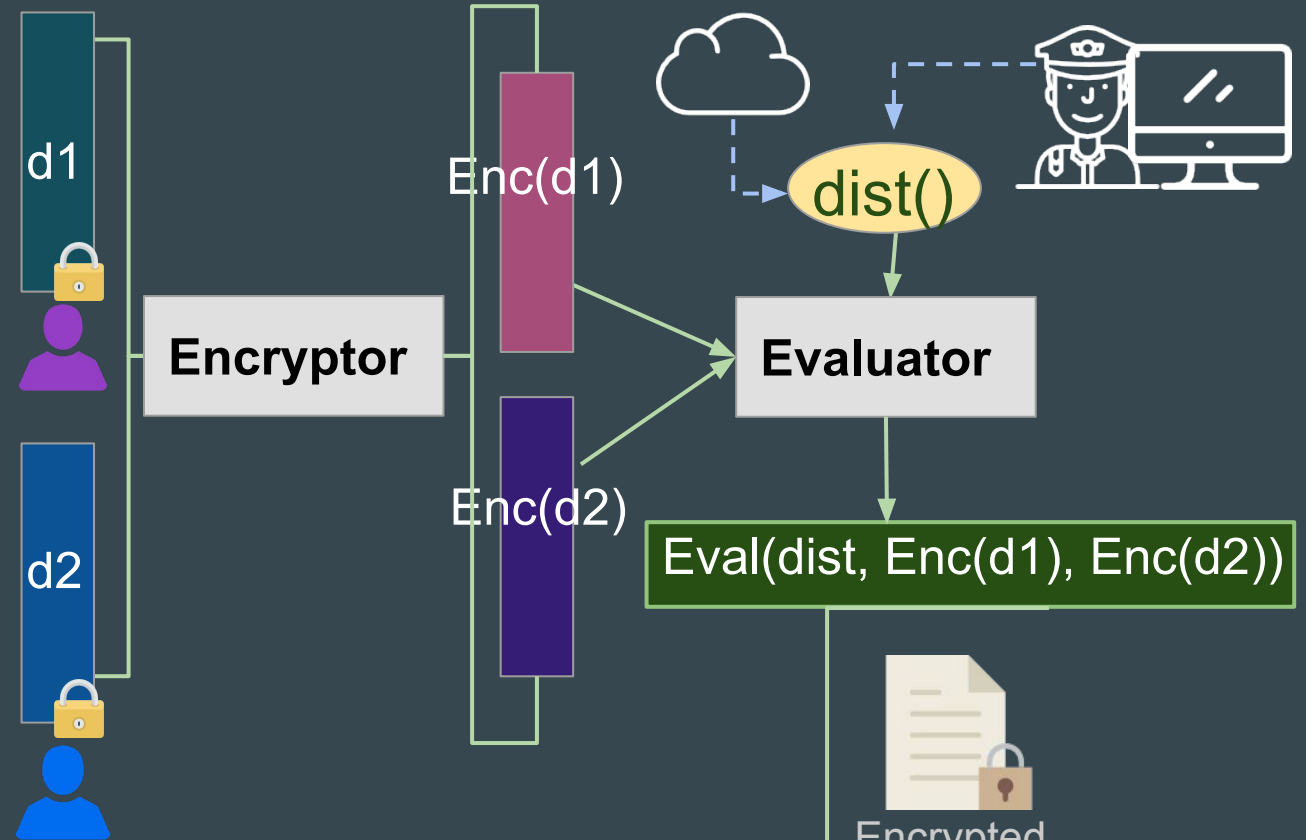
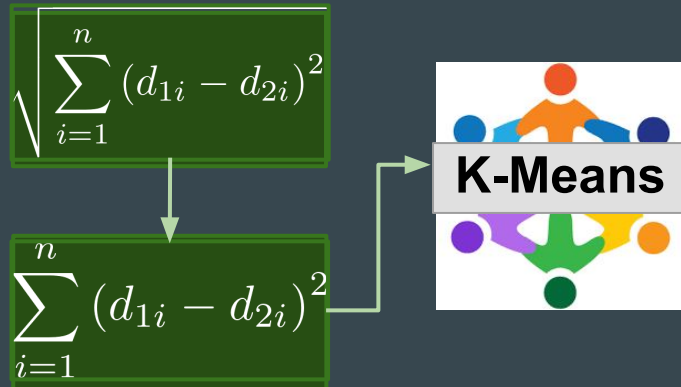
PySEAL

Python Wrapper
for the SEAL

Secure Computation Based on Homomorphic Encryption

Homomorphic similarity function:

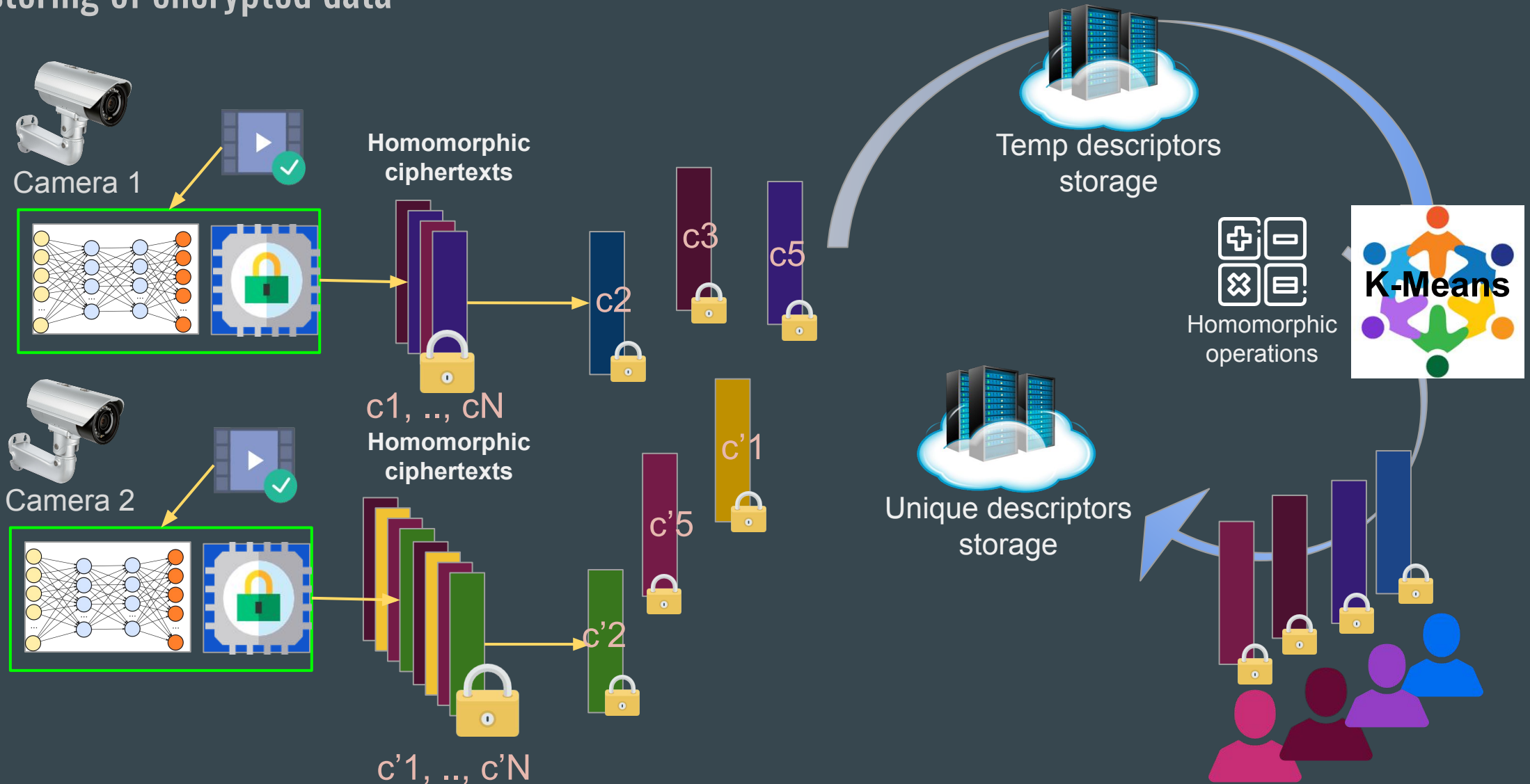
- K-Means clustering algorithm over encrypted descriptors of faces
- Search over descriptors



Decryption

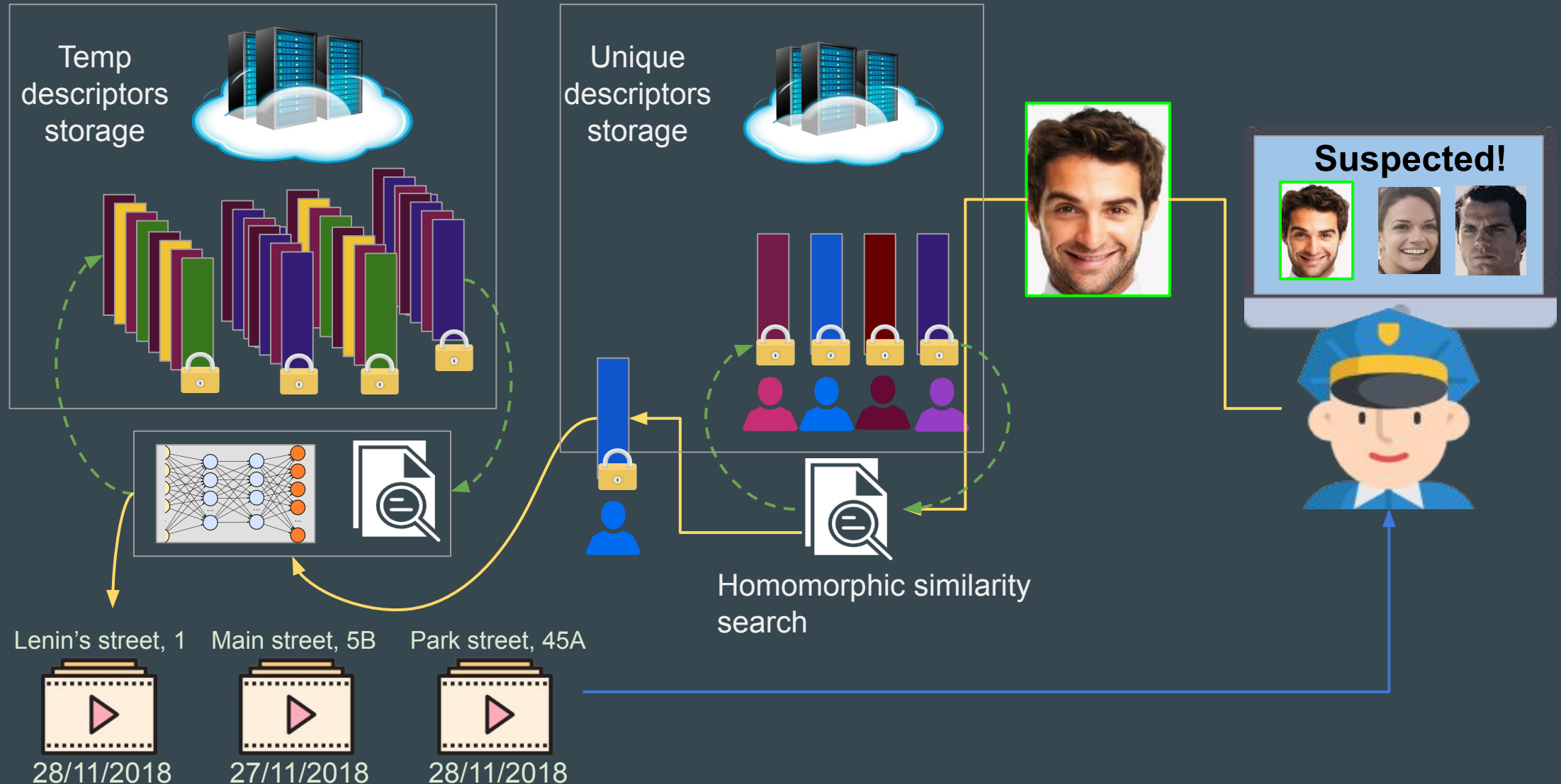
Homomorphic Encryption Module

Clustering of encrypted data

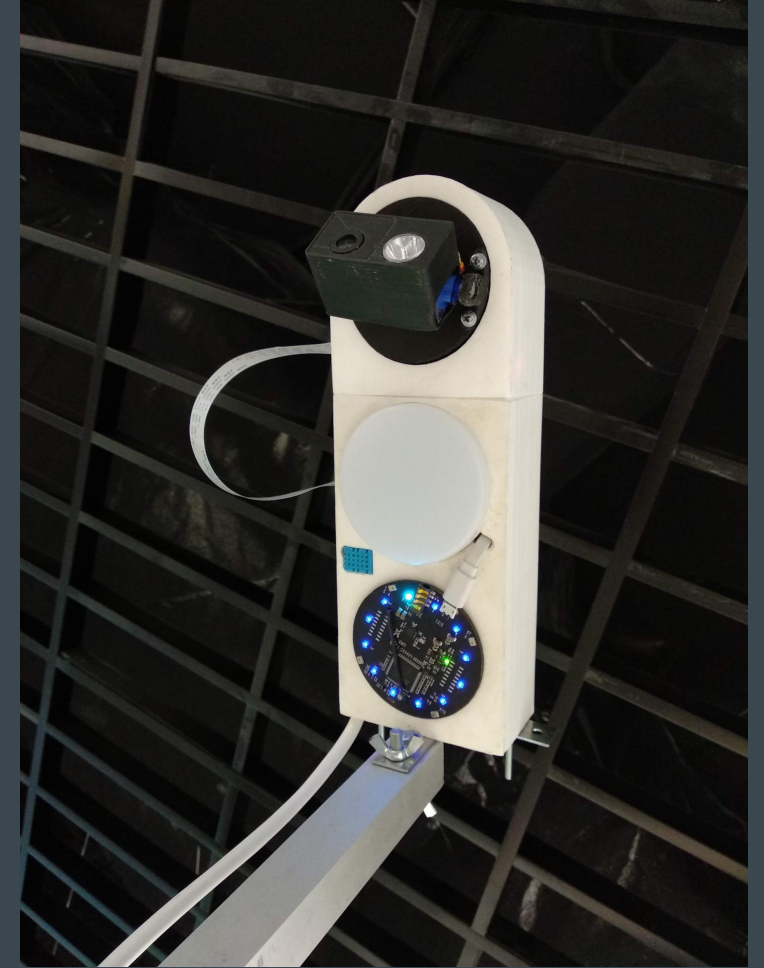


Homomorphic Encryption Module

Similarity search in faces database



3D-printed Crime Camera station



Video Management System

