End-to-End Confidentiality with SEV-SNP Leveraging In-Memory Storage

8th Workshop on System Software for Trusted Execution (SysTEX 2025)
Co-located with EuroS&P

Lorenzo Brescia (II year PhD candidate, **UniTO**)
Iacopo Colonnelli (Assistant Professor, **UniTO**)
Valerio Schiavoni (Full Professor, **UniNE**)
Pascal Felber (Full Professor, **UniNE**)
Marco Aldinucci (Full Professor, **UniTO**)

4 July 2025, SysTEX'25, Venice (IT)

ICSC
Centro Nazionale di Ricerca in HPC,
Big Data and Quantum Computing

UNIVERSITÀ DI TORINO

unine
Université de Neuchâtel
Institut d'informatique

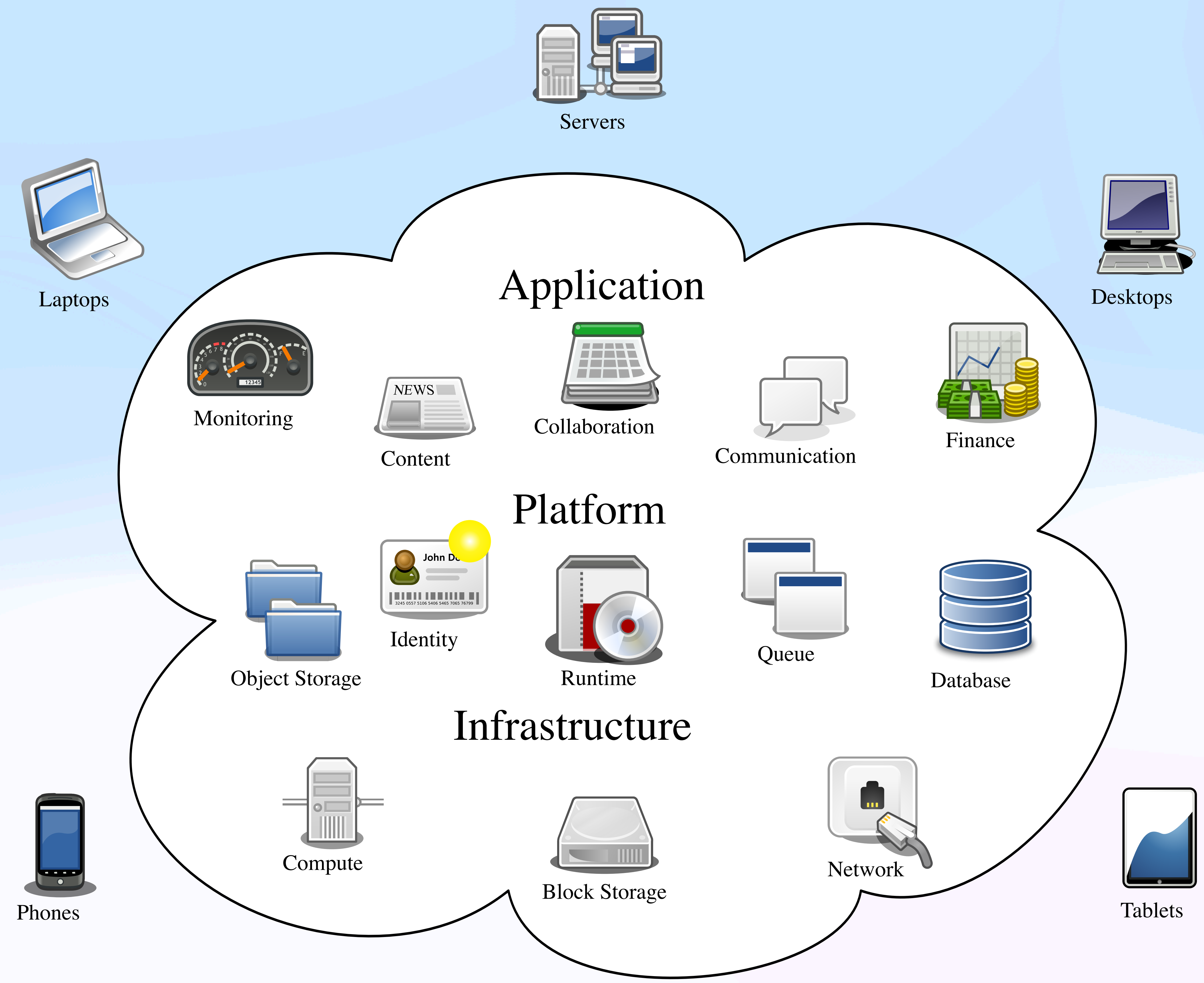
Outline

1. Background
2. Goal definition
3. Methodology
4. Discussion on results
5. Limitations future works and conclusions

Background

Cloud computing is beneficial

- Cost efficiency
- Scalability
- Accessibility
- Seamless deployment
- Trivial management

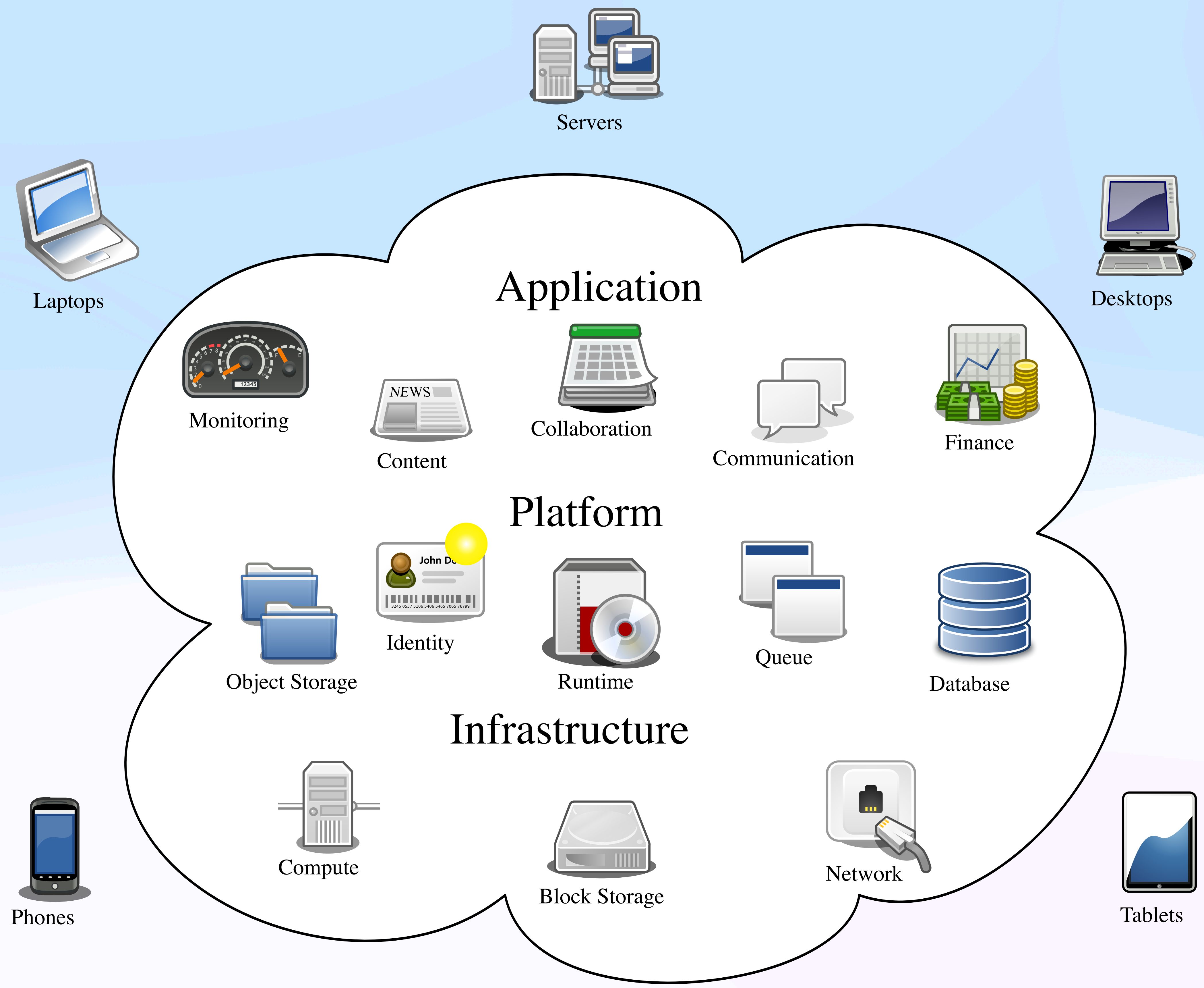


***

*** Sam Johnston - This unspecified vector graphic according to W3C was created with Inkscape, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=6080417

Cloud computing is ~~beneficial~~ opaque

- Cost efficiency
- Scalability
- Accessibility
- Seamless deployment
- Trivial management

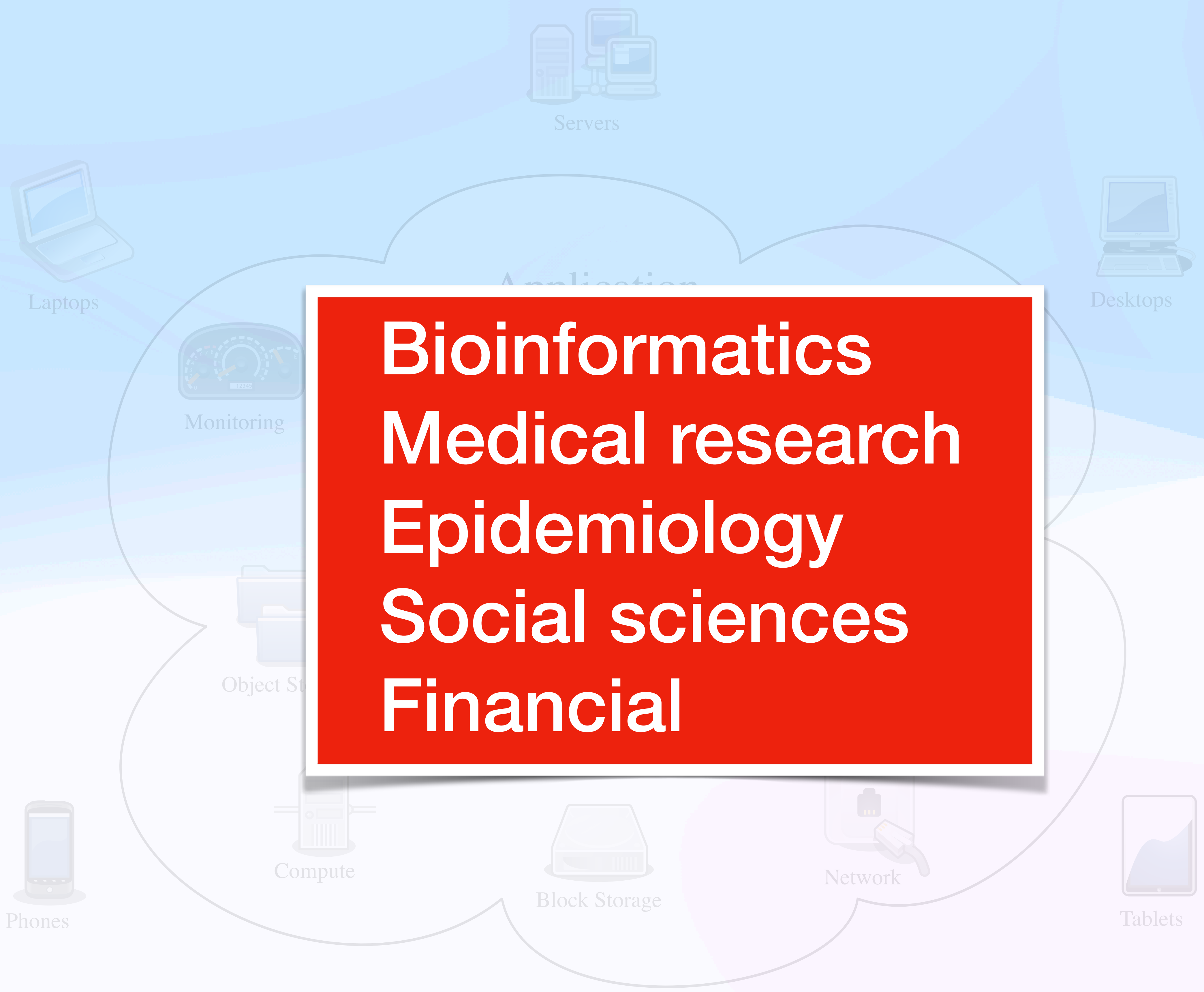


***

*** Sam Johnston - This unspecified vector graphic according to W3C was created with Inkscape, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=6080417

Cloud computing is ~~beneficial~~ opaque

Limited control
Security and privacy risks



Bioinformatics
Medical research
Epidemiology
Social sciences
Financial

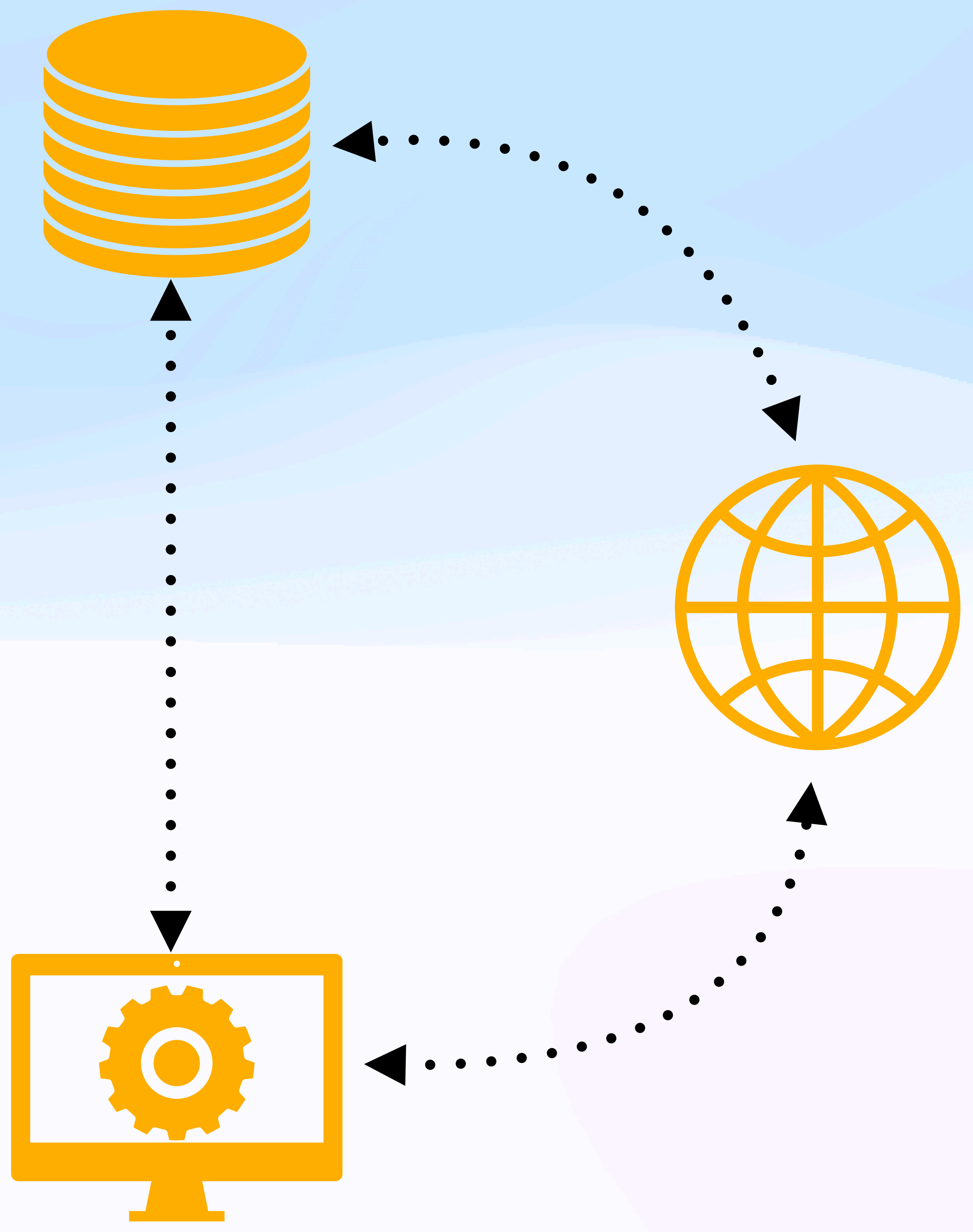
***

End-to-end data protection

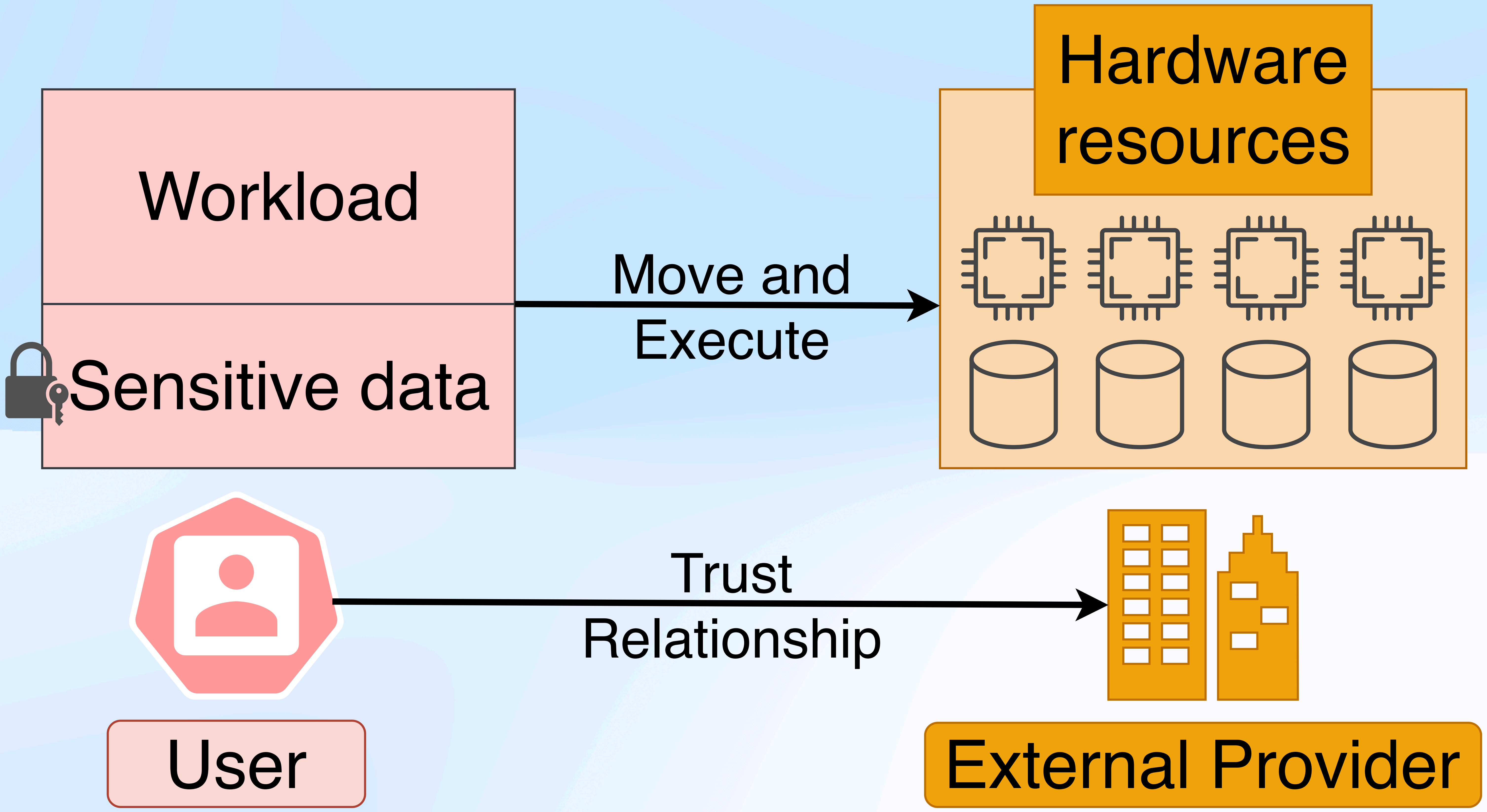
1. at-rest: storage
   (e.g., Full Disk Encryption)

2. in-transit: during transmission
   (e.g., secure channel TLS or SSH)

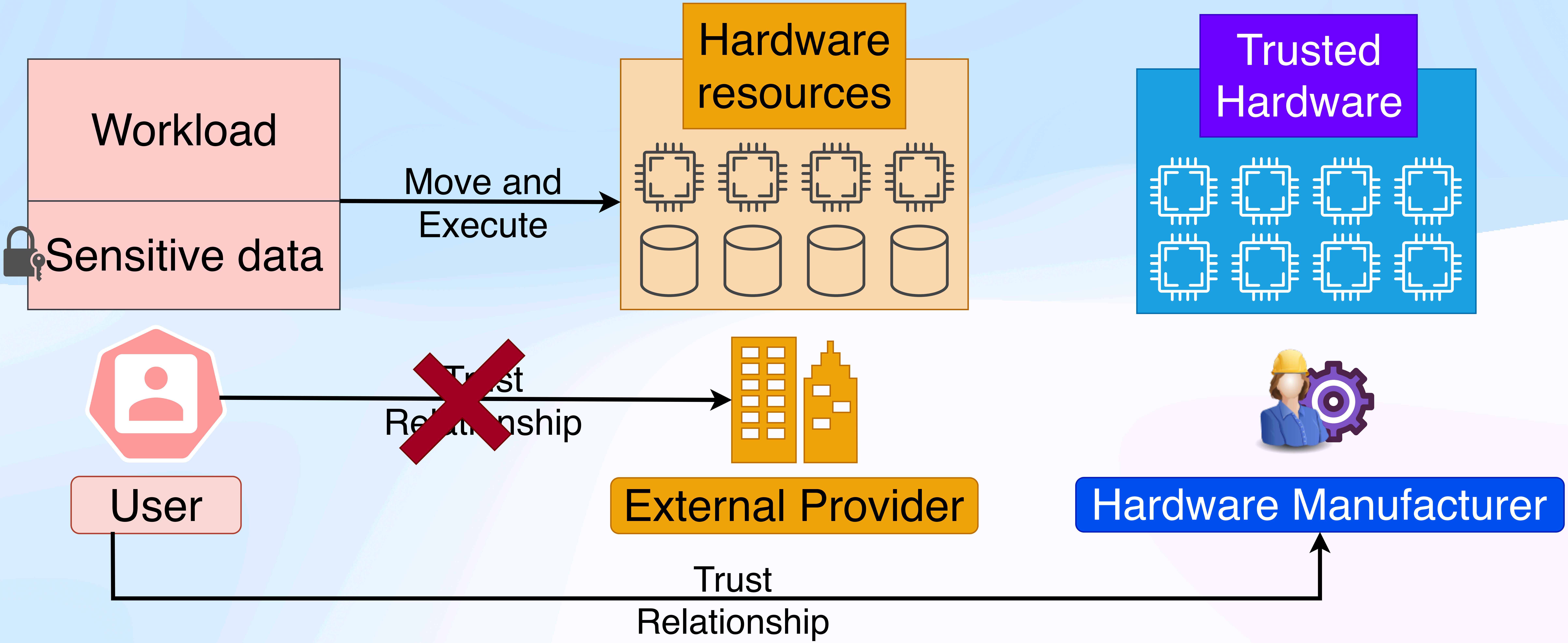
3. in-use: main memory
   (e.g., confidential computing)



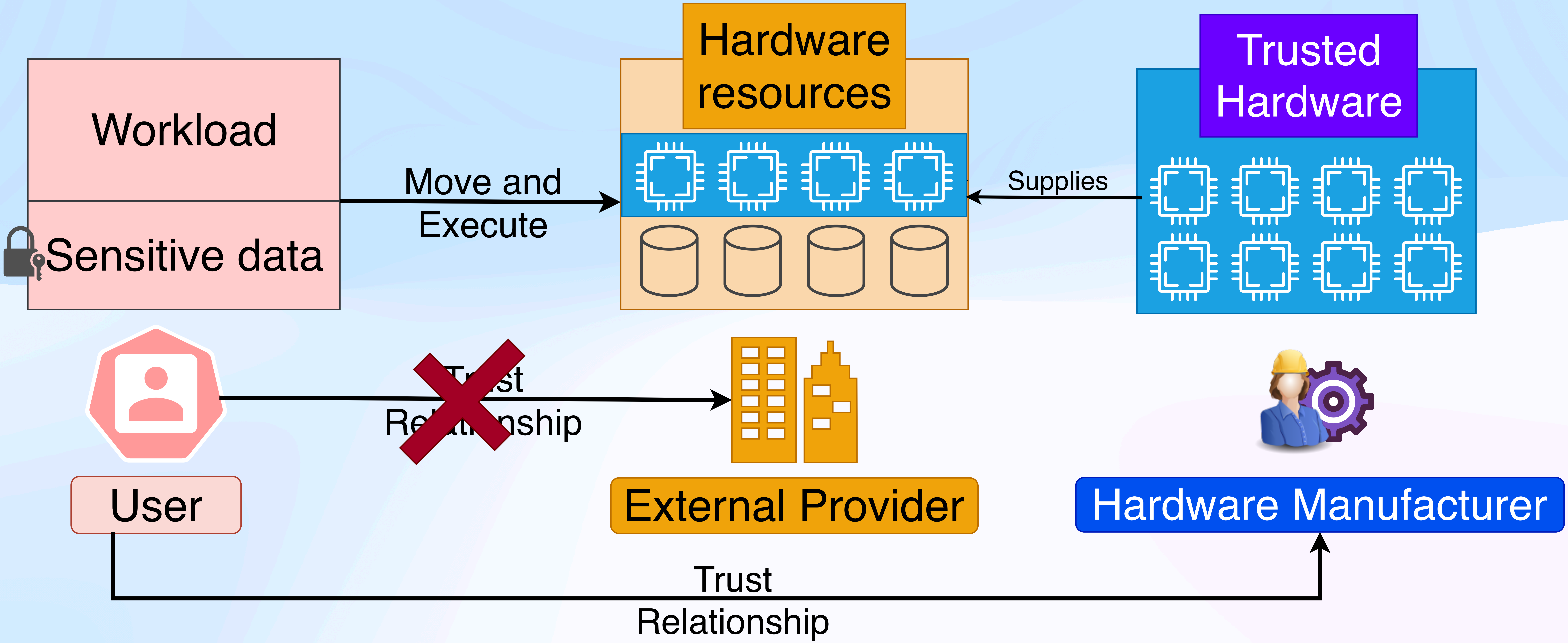
Confidential Computing



Confidential Computing



Confidential Computing

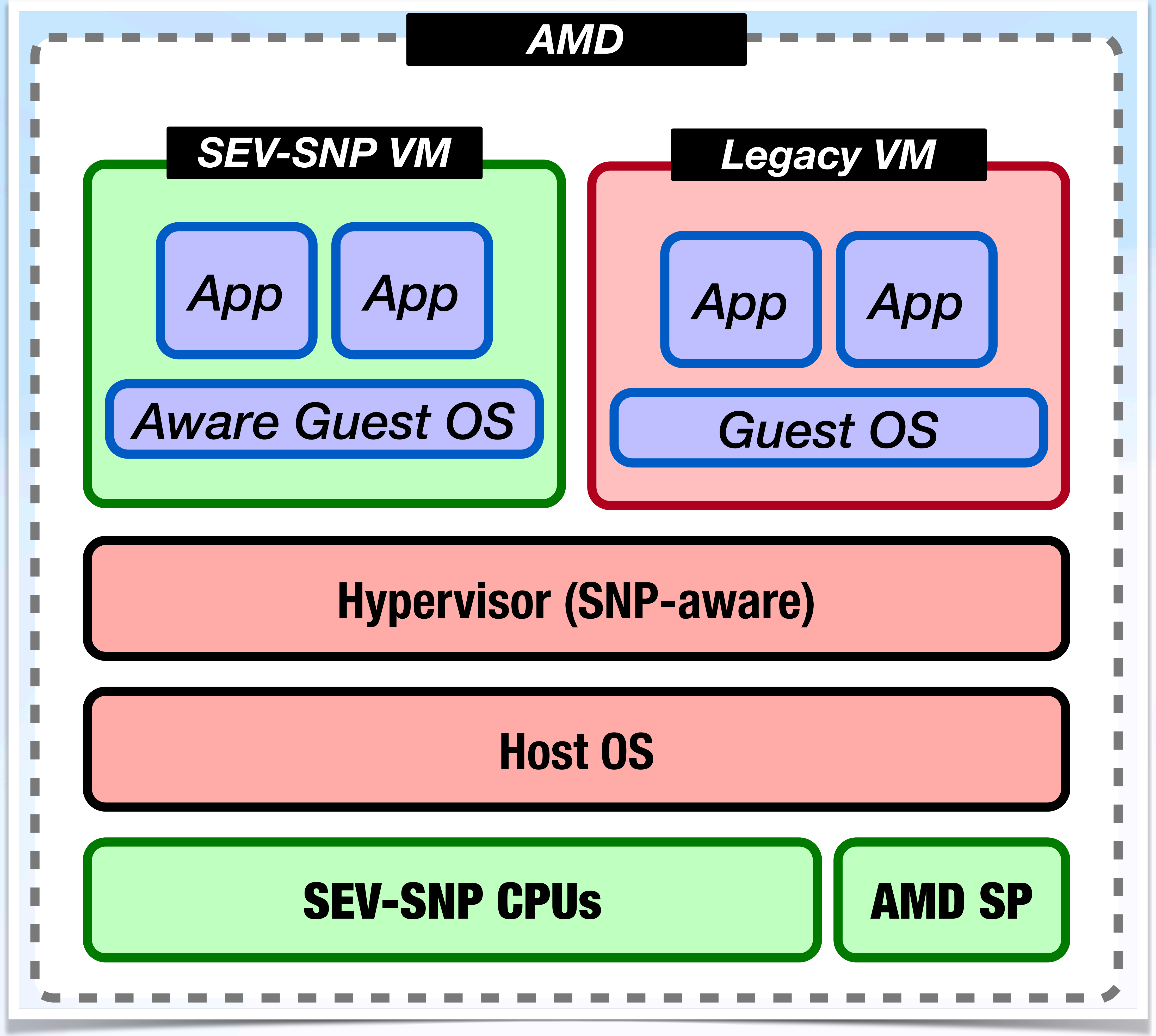


Trusted hardware vendors

- Intel SGX and TDX
- Arm Trustzone and CCA
- AMD SEV, SEV-ES and SEV-SNP
- IBM Secure Execution for Linux
- NVIDIA's Hopper GPUs
- ...

Trusted Execution Environment (TEE)

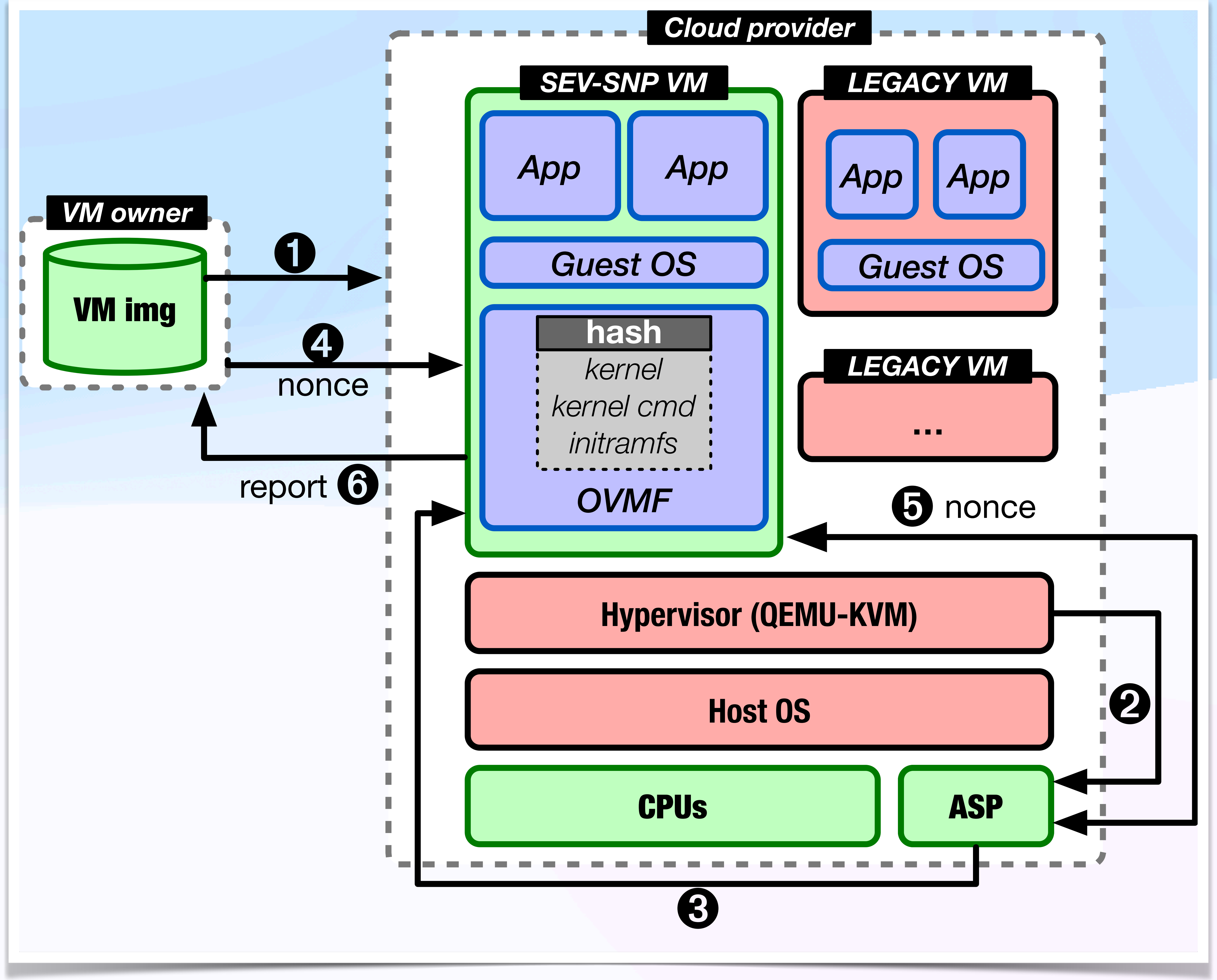
Code and data **privacy** with **integrity**



Remote attestation

Authenticate TEE, in AMD SEV:

1. VM owner provides the image
2. HV ask ASP to init. the VM pages
3. Measurement (OVMF, kernel, intiramfs, cmd line)
4. VM owner sends a nonce
5. VM requests report to ASP
6. VM forwards the report to VM owner



Goal

Maintain E2E data protection while reducing the overhead associated with FDE by leveraging in-memory storage solutions inherently protected TEE

Methodology

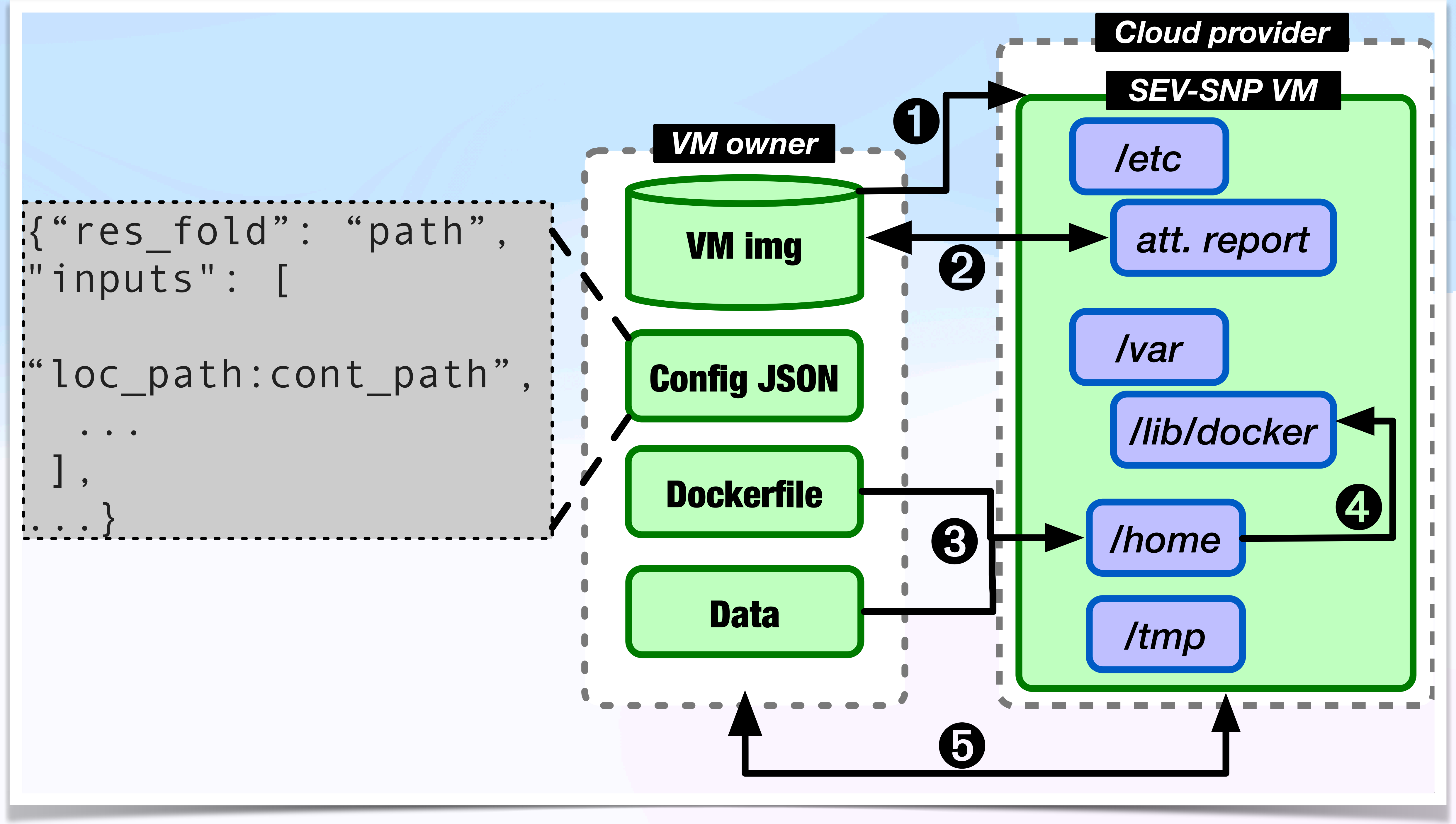
SNPGuard

Open-source solution for boot SEV-SNP VMs in two modes:

1. Confidentiality + Integrity
    - VM image encrypted with LUKS
    - VM image unlocked during initramfs after attestation
2. Integrity
    1. VM image with a read-only non confidential disk
    2. /home, /etc, /var and /tmp mounted as tmpfs
    3. VM integrity verified during initramfs phase
    4. Attestation report in tmpfs

E2E confidentiality execution flow

1. Launch VM with SNPGuard integrity mode
2. Retrieve and validate report
3. Move data and Dockerfile in the VM
4. Docker build and Docker run
5. Results retrieve (if any)



FDE

E2E confidentiality guaranteed
In-use: TEE
At-rest: FDE
In-transit: SSH channels

In-memory storage

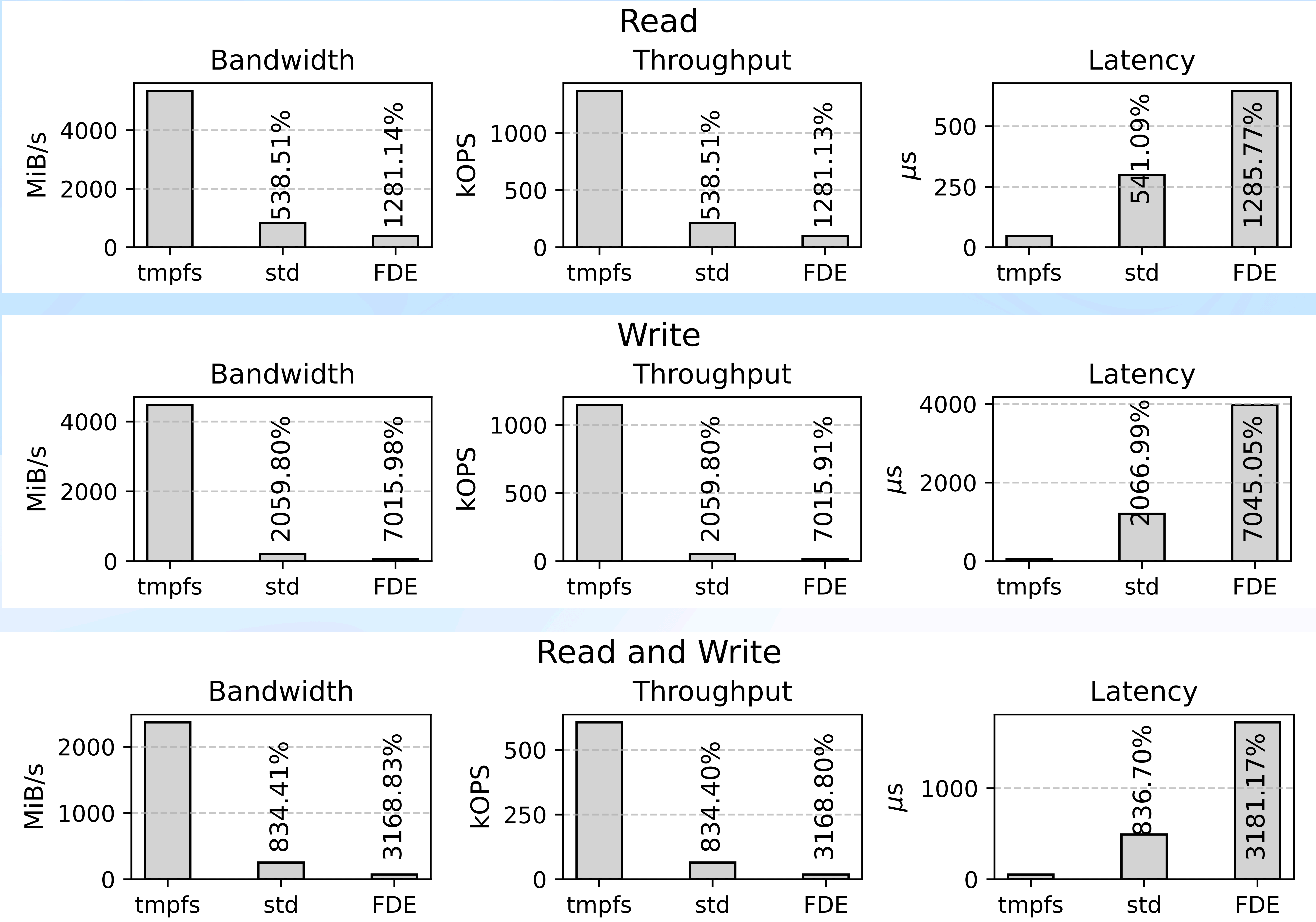
E2E confidentiality guaranteed
In-use: TEE
At-rest: TEE
In-transit: SSH channels

Results

Testbed

Category	**Component**	**Specification**
Host System	CPU	AMD EPYC 9124 (16 cores, 32 threads, SMT)
	RAM	66 GiB
	Storage	512 GB SSD
	OS (Host)	Ubuntu 22.04.5
	Kernel (Host)	6.9.0-rc7-snp-host-05b10142ac6a
VMs (All)	vCPUs	32
	RAM	32 GiB
	Disk	70 GB (scsi-hd)
	OS (Guest)	Ubuntu 22.04.5
	Kernel (Guest)	6.9.0-snp-guest-a38297e3fb01
	Software Stack	Identical (e.g., Docker)
VM Variants	**std**	**Standard** SEV-SNP VM
	FDE	SEV-SNP VM using **LUKS Full Disk Encryption**
	tmpfs	SEV-SNP VM using **tmpfs-mounted directories**

fio: disk microbenchmarks



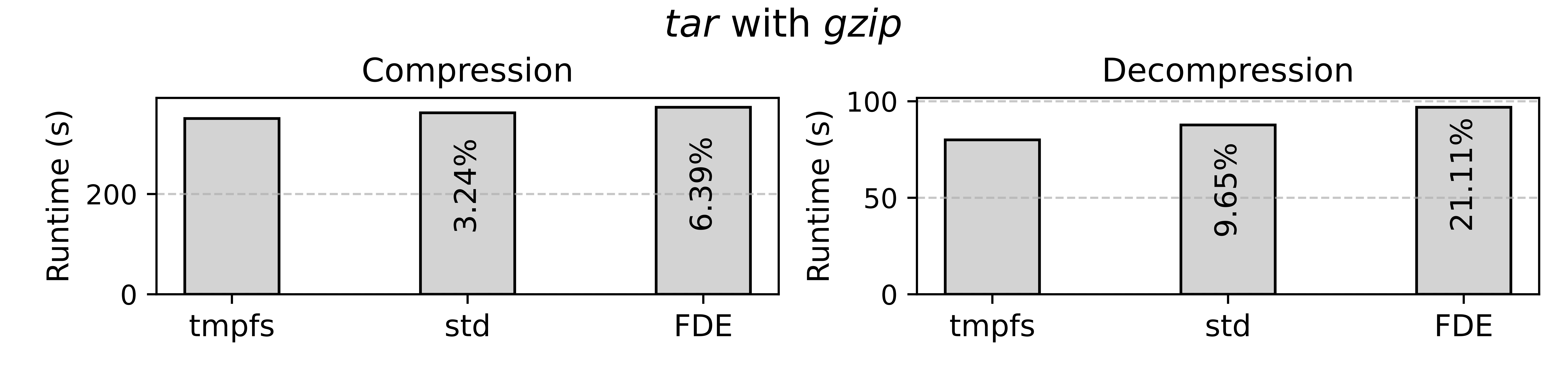
Read 13x

Write 70x

Mixed 30x

Performance drops with FDE also compared STD

Compression and Decompression workload

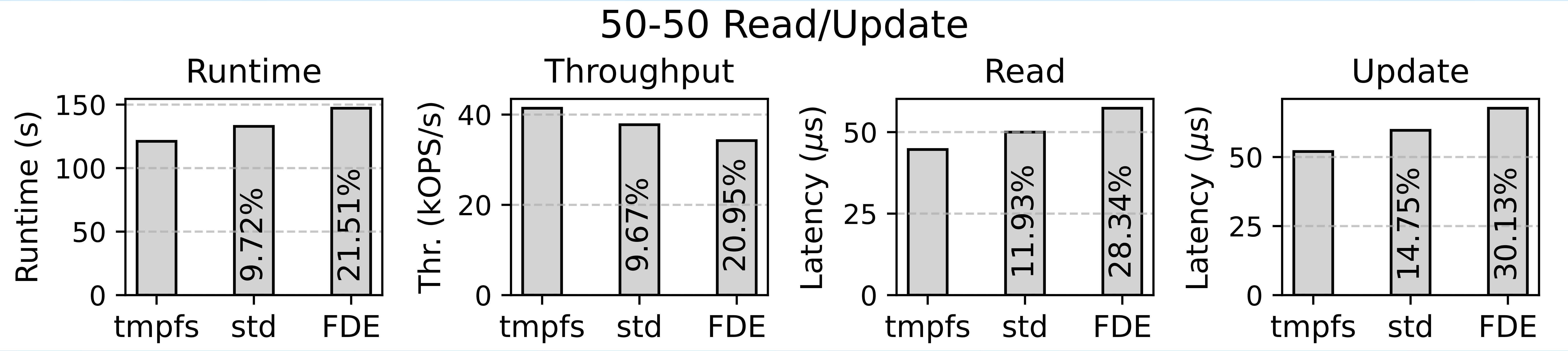


- 10 GB from an open dataset of human action video clips
- Compression is CPU-bound
- Decompression is disk-bound

Compression 6%

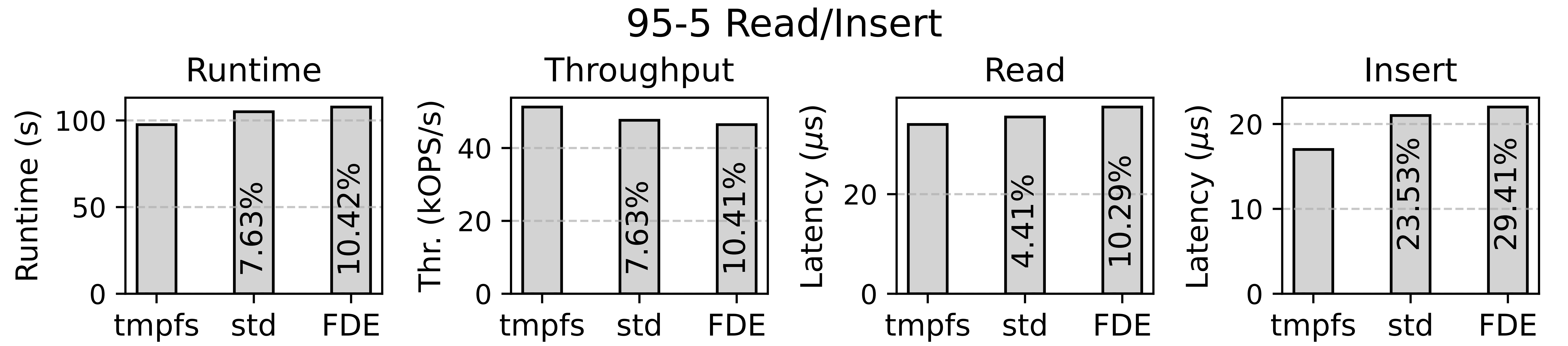
Decompression 21%

Database workload YCSB (1)



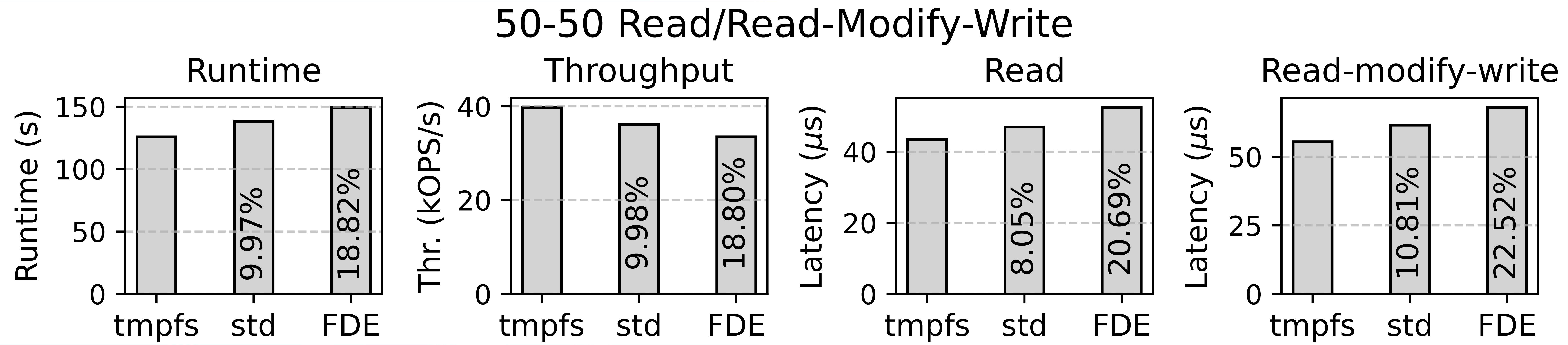
Thr: 20%

Lat: 28-30%



Thr: 10%

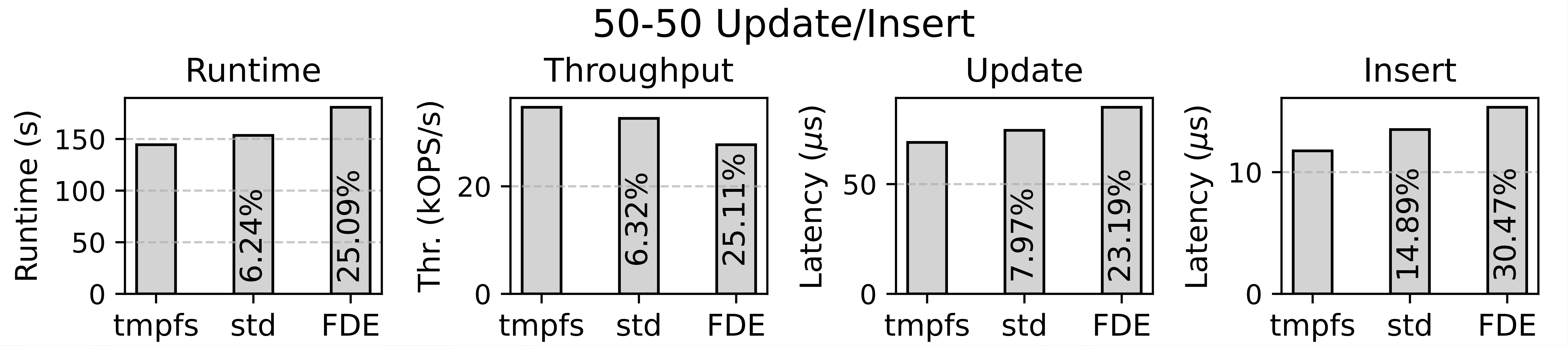
Lat: 10-29%



Thr: 18%

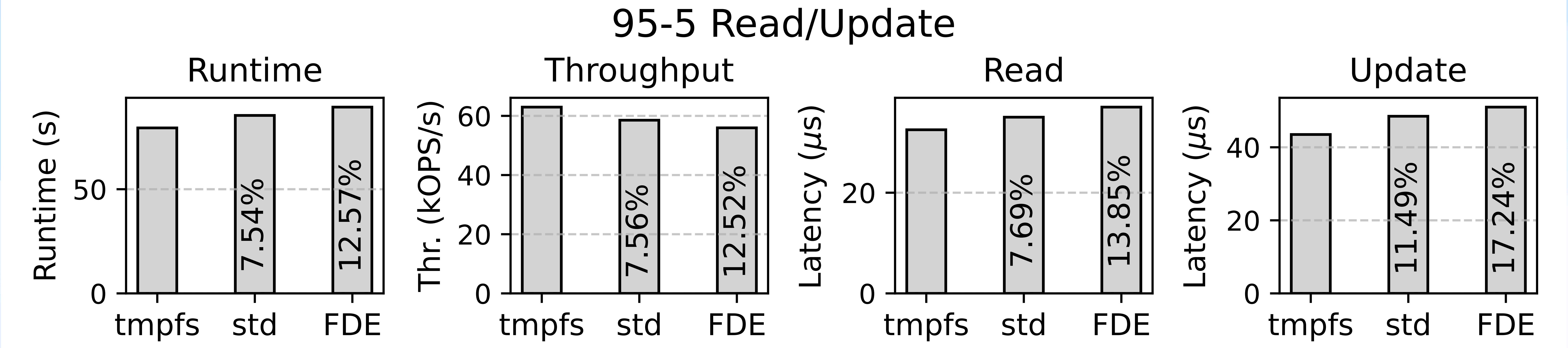
Lat: 20-22%

Database workload YCSB (2)



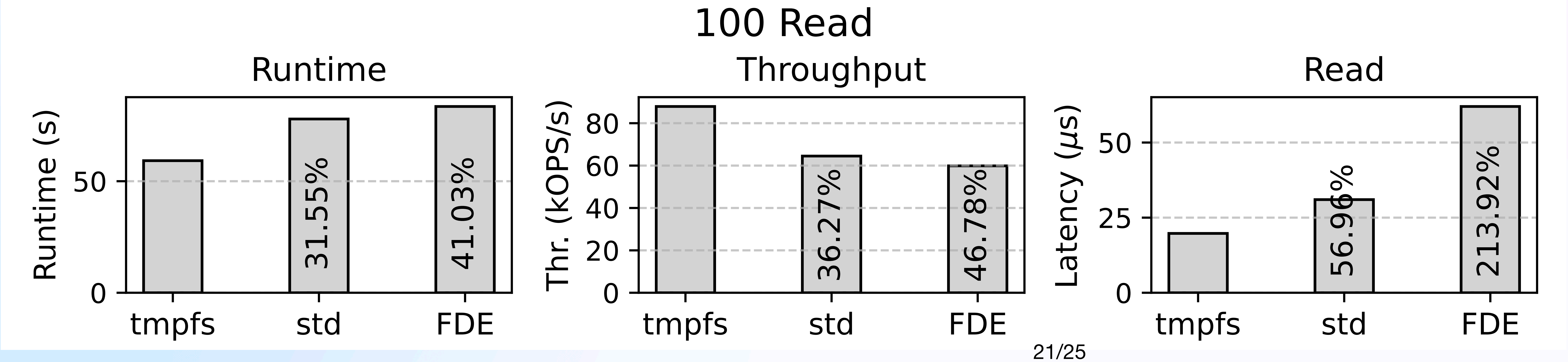
Thr: 25%

Lat: 23-30%



Thr: 12%

Lat: 13-17%



Thr: 46%

Lat: 213%

Conclusions

Limitations due to volatility

1. Memory is more expensive than disk storage
2. Failures can cause loss of in-memory intermediate results
3. Limited memory capacity can restrict data size and halt computation

Future work

1. Fault tolerance mechanism (with checkpoint)
2. Expand for other VM-based TEEs (e.g. TDX)
3. Improve quality of the assessment (e.g. Docker)

Final remarks

1. FDE can introduces significant overhead in storage-intensive workloads
2. Our framework provides:
    1. End-to-end data protection
    2. Up to 45% (avg. 20%) performance gain over FDE
3. Read-only workloads benefit most - no need to persist results after execution

Personal page

ICSC
Centro Nazionale di Ricerca in HPC,
Big Data and Quantum Computing

UNIVERSITAS STUDII TAURINENSIS 1404
UNIVERSITÀ DI TORINO

unine
Université de Neuchâtel
Institut d'informatique

Lorenzo Brescia (II year PhD candidate, **UniTO**)
Iacopo Colonnelli (Assistant Professor, **UniTO**)
Valerio Schiavoni (Full Professor, **UniNE**)
Pascal Felber (Full Professor, **UniNE**)
Marco Aldinucci (Full Professor, **UniTO**)

4 July 2025, SysTEX'25, Venice (IT)