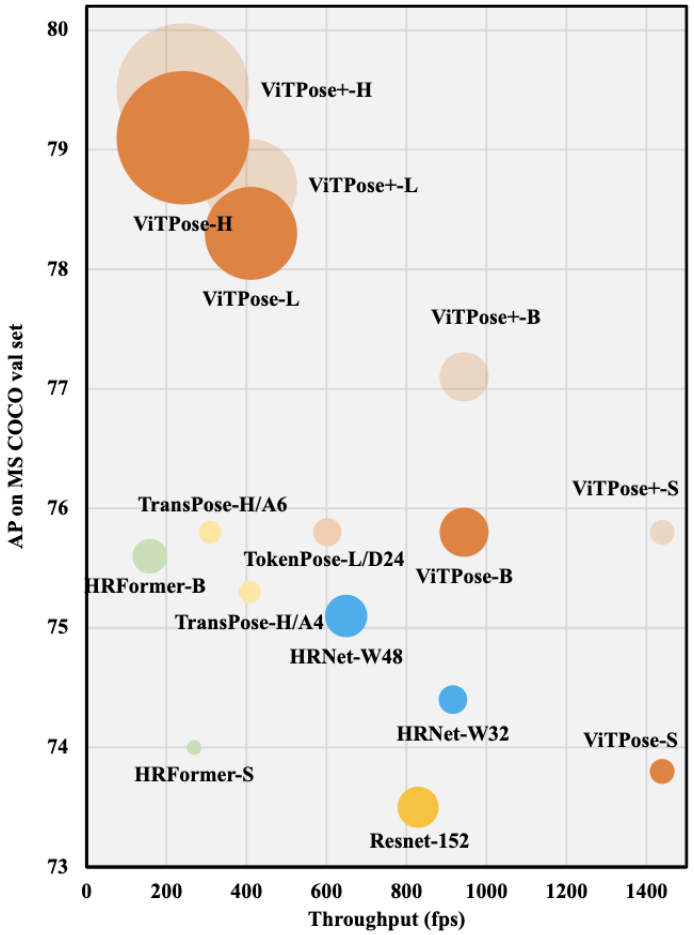
Don’t call it *privacy-preserving* or *human-centric* pose estimation if you don’t measure privacy

Michele Baldassini, Francesco Pistolesi, and Beatrice Lazzerini

Department of Information Engineering
University of Pisa, Italy

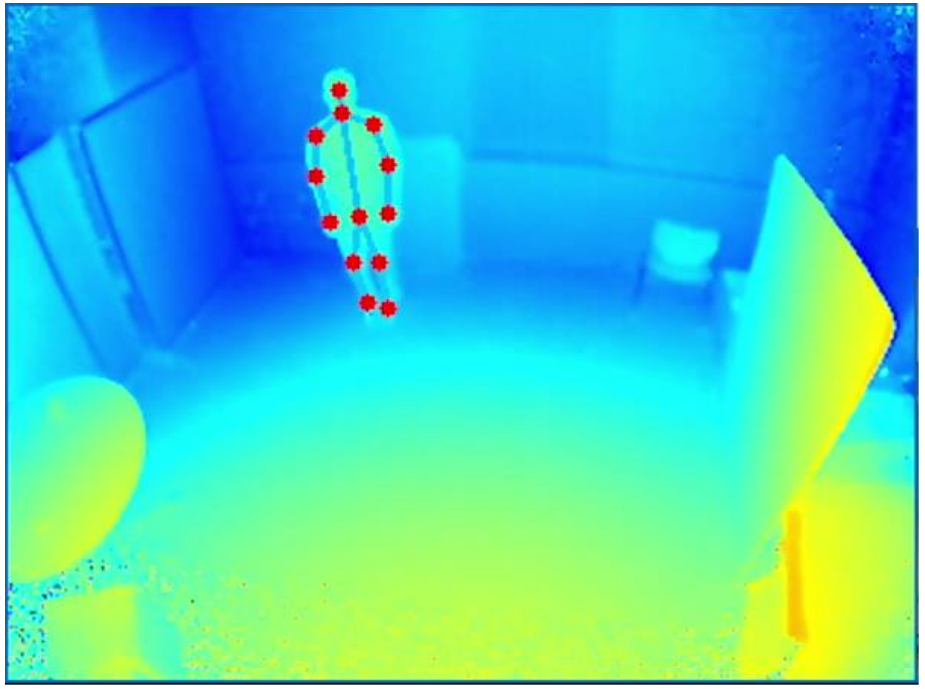
michele.baldassini@ing.unipi.it, francesco.pistolesi@unipi.it, beatrice.lazzerini@unipi.it

Overview


AP on MS COCO val set
Throughput (fps)
80
79
78
77
76
75
74
73
0
200
400
600
800
1000
1200
1400
ViTPose+-H
ViTPose+-L
ViTPose-H
ViTPose-L
ViTPose+-B
ViTPose+-S
TransPose-H/A6
TokenPose-L/D24
ViTPose-B
HRFormer-B
TransPose-H/A4
HRNet-W48
HRNet-W32
ViTPose-S
HRFormer-S
Resnet-152

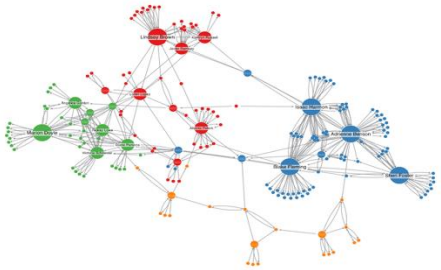

FPS: 1.4 | Pose FPS: 9.4 | Detection FPS: 1.7
CHEESE DIP
CHICKS
423-629-1990

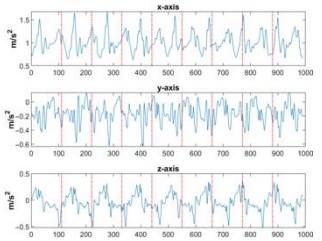
What is privacy?



Smartphones

Social networks





Temporal patterns

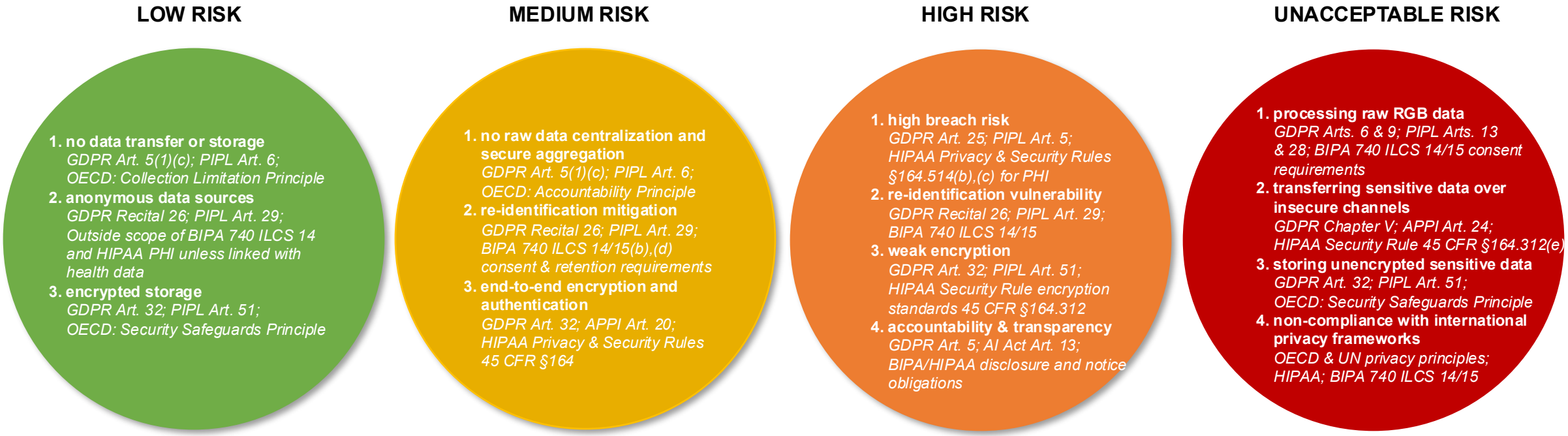
Other sensing devices

Space info

Regulations in the real world

Privacy is not optional: each domain already operates under specific laws and regulations.

Risk levels based on international privacy regulations



Dimensions

DATA SENSITIVITY	PRIVACY MEASURES	MODEL	DATA TRANSFER	DATA STORAGE
What information is included in the data?	Reducing sensitive information in the data	How the model processes data during inference/training?	Ensuring a secure transfer of sensitive information	Ensuring a secure storage of sensitive information
ASPECTS				
1. Scenario identifiability 2. Different *SPI* exposure 3. Re-identification with 3D human body modeling	1. Scene or pose data 2. Encryption / anonymization 3. Pipeline stages with privacy measures	1. Training paradigm (e.g., de-centralized, federated 2. Inference location (e.g., edge, fog, cloud)	1. Communication protocols security 2. Clear sensitive information in data 3. Encrypted data transfer?	1. Encrypted / anonymized data storage 2. Physical and logical location 3. Purpose-limited retention
RECOMMENDATIONS				
1. Reduction of scenario identifiability 2. Exposure of less relevant *SPI* 3. Mitigation of re-identification	1. Encryption & anonymization 2. Retention of pose data only 3. Privacy measure at edge node	1. De-centralized or federated training 2. Inference at edges nodes	1. Secure communication protocols (e.g., TLS, IPSec) 2. No sensitive information transfer 3. Strong encryption	1. Storage of encrypted data 2. Limited exposure of data (e.g., edge nodes) 3. Limited retention of data

Sensing modality

PROS
- Does not capture facial texture
- Works in low light or darkness

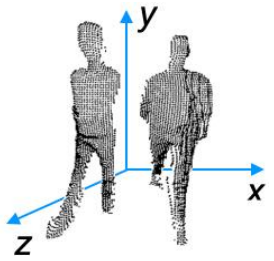
CONS
- Many leaks physiological traits
- Limited structural details
- Requires expensive sensors

PROS
- Reduces identifiers
- Provides reliable spatial structure
- Widely supported (e.g., Kinect)

CONS
- Encodes body shape and size
- Sensitive to lighting
- May struggle with occlusions and outdoor environments

PROS
- Easy to build on RGB streams
- Preserves spatial layout and coarse motion cues
- Reduces recognizability

CONS
- Degrades keypoint accuracy
- Faces or bodies may remain partially recognizable



PROS
- Accurate spatial information
- No visual texture
- Resilient to lighting conditions

CONS
- Reveals body geometry
- High cost and complexity
- Not suited for fine-grained movement analysis

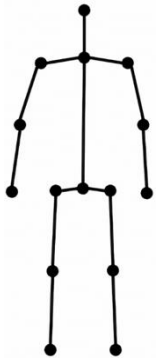
PROS
- Abstracts away color and texture
- Preserves posture lines
- Lightweight representation

CONS
- May leak structural identity
- No depth information
- Hard to apply to dynamic scenes

PROS
- Strong obfuscation of details
- Maintains approximate pose
- Efficient preprocessing step

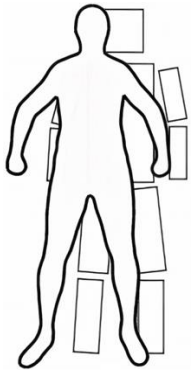
CONS
- Level of obfuscation depends on pixel size and distance
- Can leak body silhouette
- Degrades HPE performance

Pose data



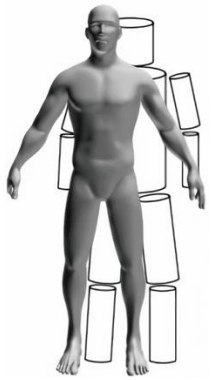
- Minimizes personal identifiability
- Hides physical appearance

- Hides facial details
- Preserves motion and spatial context



- Exposes pose or motion patterns
- Possible re-identification if combined with other data

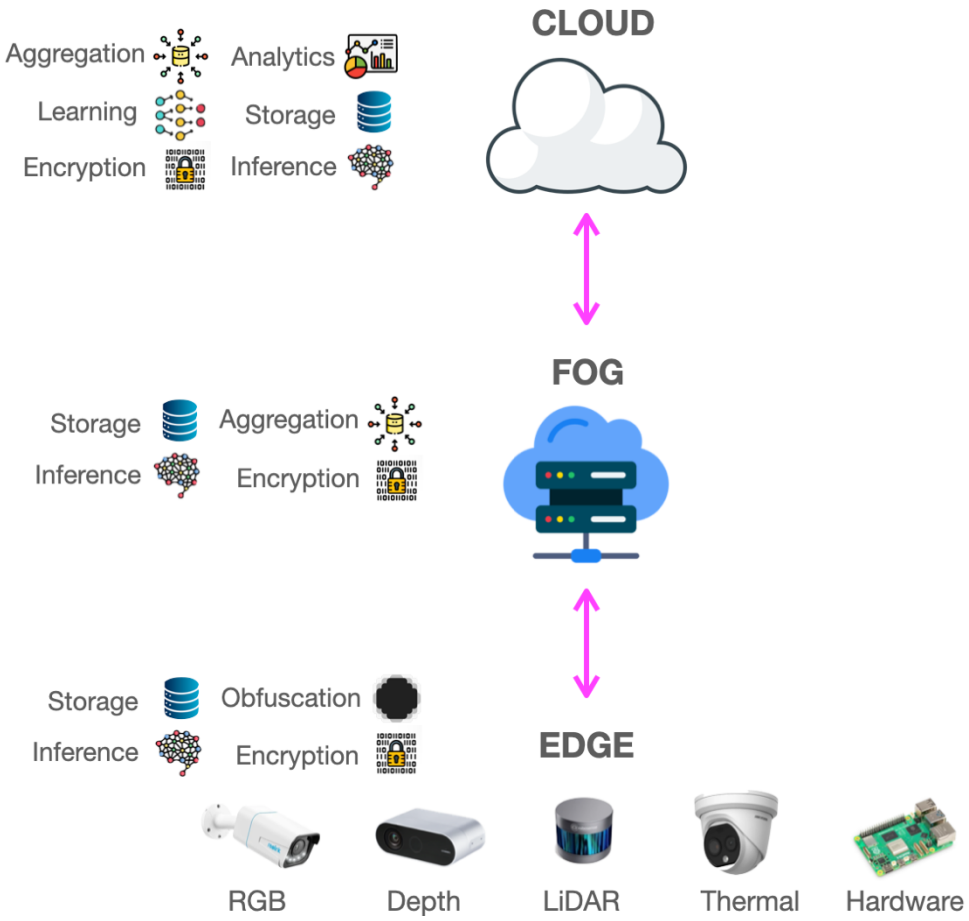
- Reveals body shape and size
- Enables indirect identification

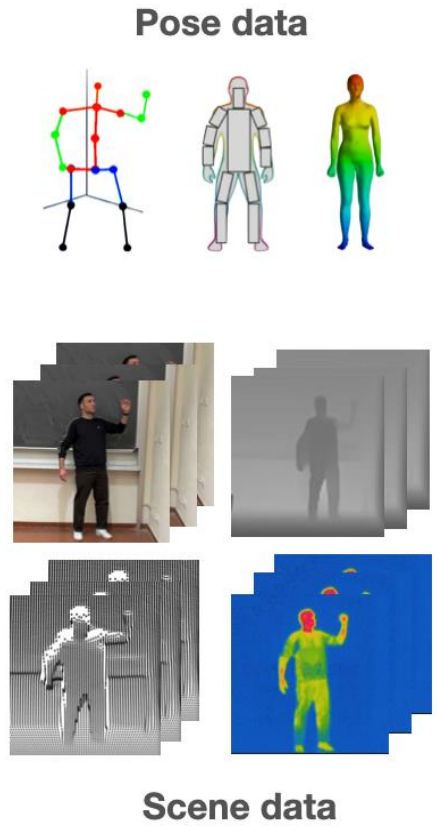


- Supports detailed analysis with partial anonymity
- Can be anonymized with abstraction methods

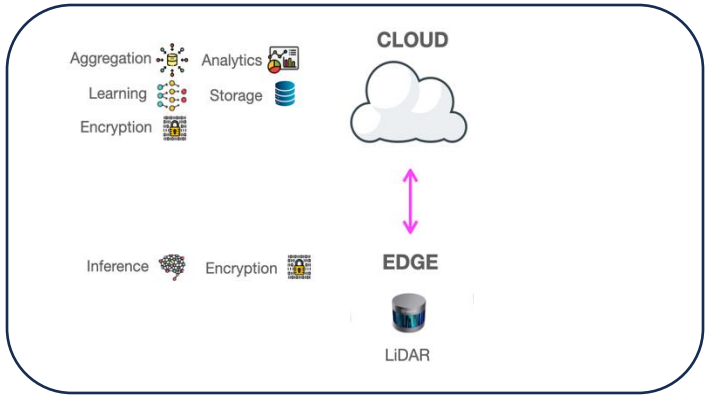
- Contains rich biometric information
- High re-identification risk

Distributed HPE deployments

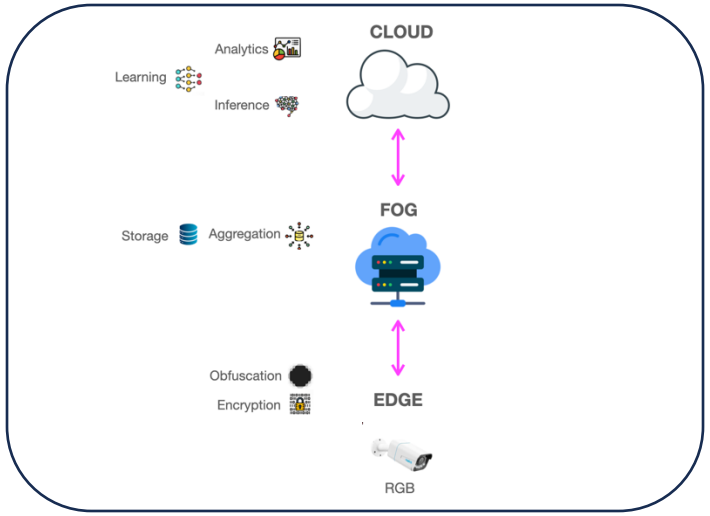




Examples



- RGB data are collected, stored in the cloud, possibly reused or shared without consent



- Data are processed locally, anonymized or obfuscated, and not stored or transmitted.

Current trends

Privacy is difficult to measure

Synthetic or augmented data preserve privacy

Switching to non-RGB data guarantees privacy

Privacy-preserving means not storing or transferring data

Potential risk indicators

How sensitive are the input data?

Privacy score

Scores the input data type

How many risky tasks in the pipeline?

Pipeline penalty

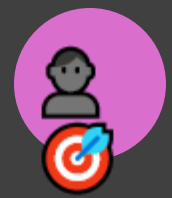
Adds a penalty for every step in the processing pipeline.

Is it compliant with GDPR / AI Act / PIPL?

Legal label

Shows the system's compliance with data protection laws.

Can a person be identified again from the output?



Re-ID test

Evaluates re-identification risk using deep learning–based ReID models.

Conclusions

Privacy should be:

- A **measurable** property.
- **Multi-dimensional** (data, models, pipeline).
- Integrated from the **design** stage and used in forthcoming benchmarking tools