Si Zuo, Stephan Sigg

Usable security enhancements on smart devices
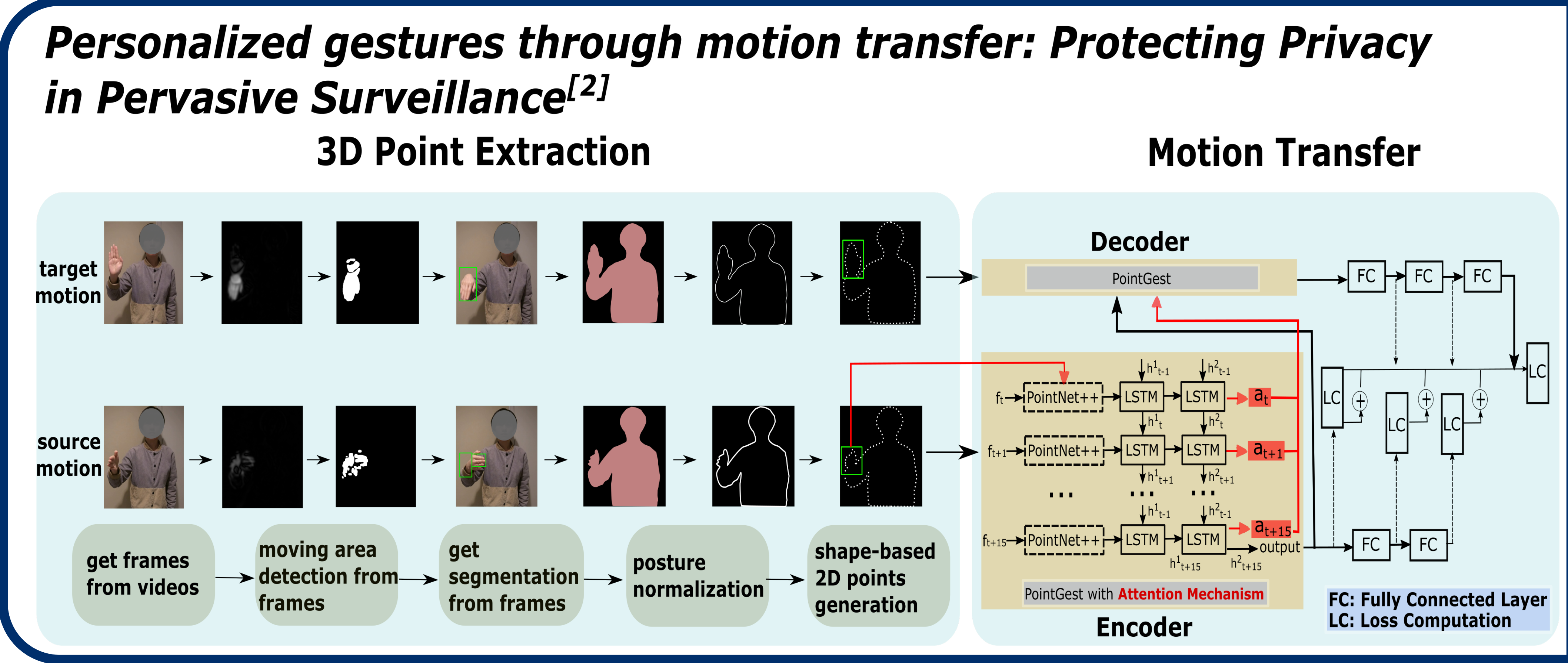
CardioID: Secure ECG-BCG agnostic interaction-free device pairing[1]

obtain signals from BCG and ECG sensors

"clean" the BCG / ECG signals

detect key points of heartbeats

compute features from key points (*heart-rate variability*)

transform features into Gray encoded fingerprints

compute secure pairing keys via fuzzy cryptography

device pairing

time interval from ECG and BCG (t_{ECG}, t_{BCG}) → t_{ECG} = 686ms t_{BCG} = 677ms

convert the numbers to hexadecimal numbers ($N_{16\text{-}ECG}$, $N_{16\text{-}BCG}$) → $N_{16\text{-}ECG}$ = 0x2ae $N_{16\text{-}BCG}$ = 0x2a5

encode the last second number of hexadecimal numbers by Gray code (G_{ECG}, G_{BCG}) → G_{ECG} = 1010 G_{BCG} = 1010

paring based on Gray code (G_{ECG}, G_{BCG})

ECG

BCG

On-body smart devices
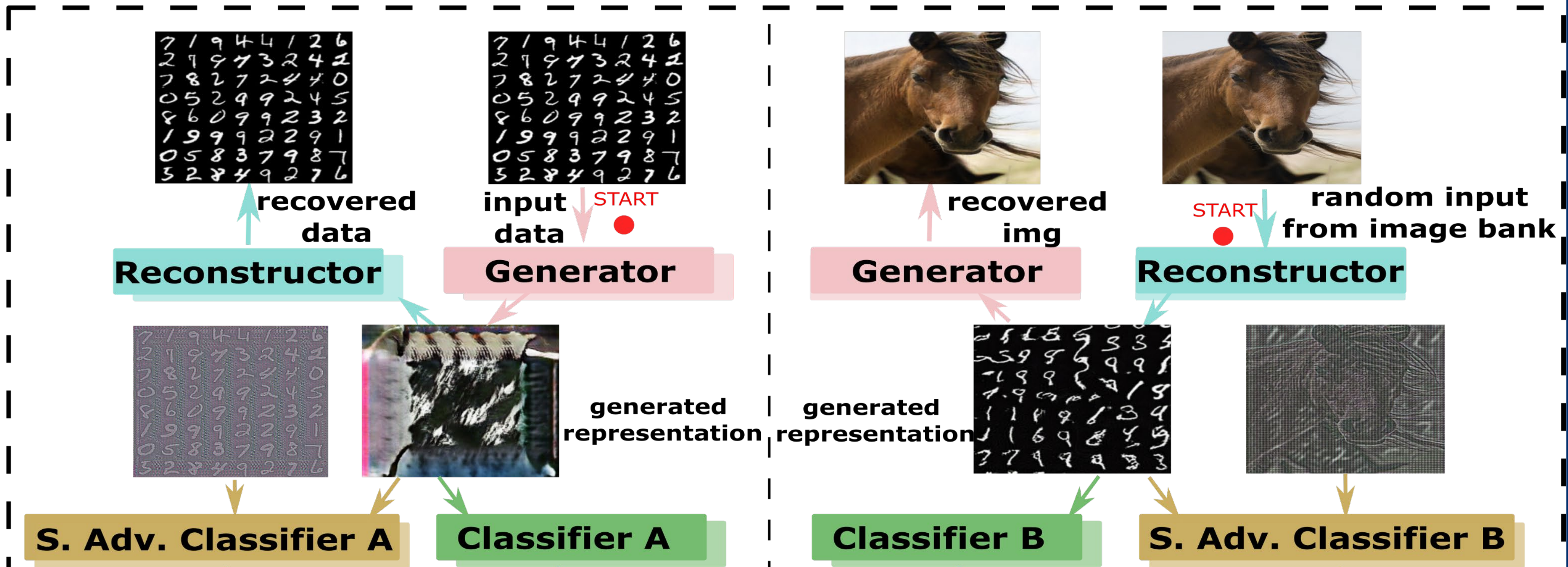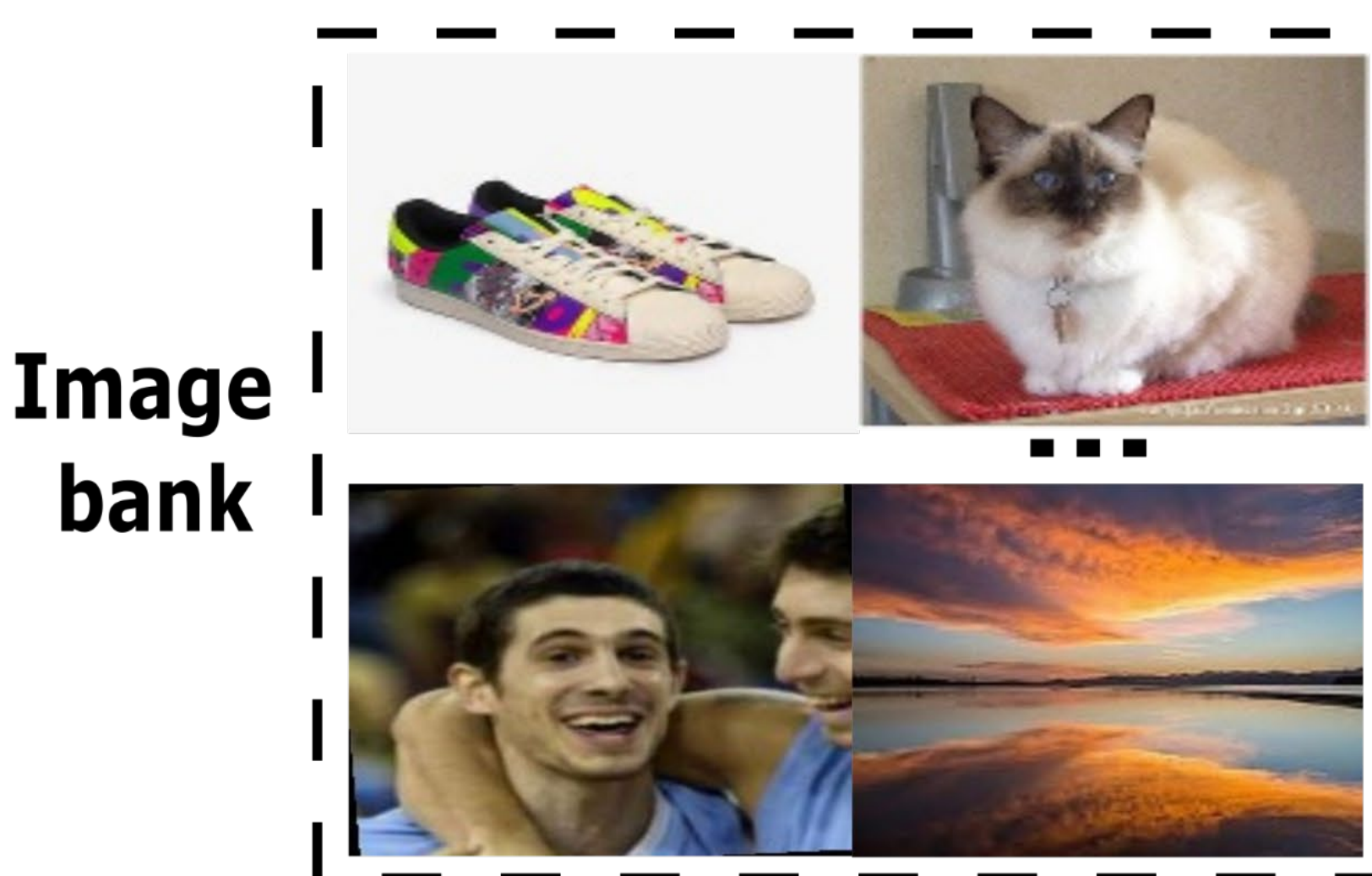
- Devices: fitness / medical wearables

- Attack: identity theft, data breach

- Solution: secure devices paring with BCG and ECG signals by extracting heart rate variability.

Interactable smart devices with gestures

- Devices: drones
- Attack: device hijacking
- Solution: personalized gestures for device control through motion transfer.

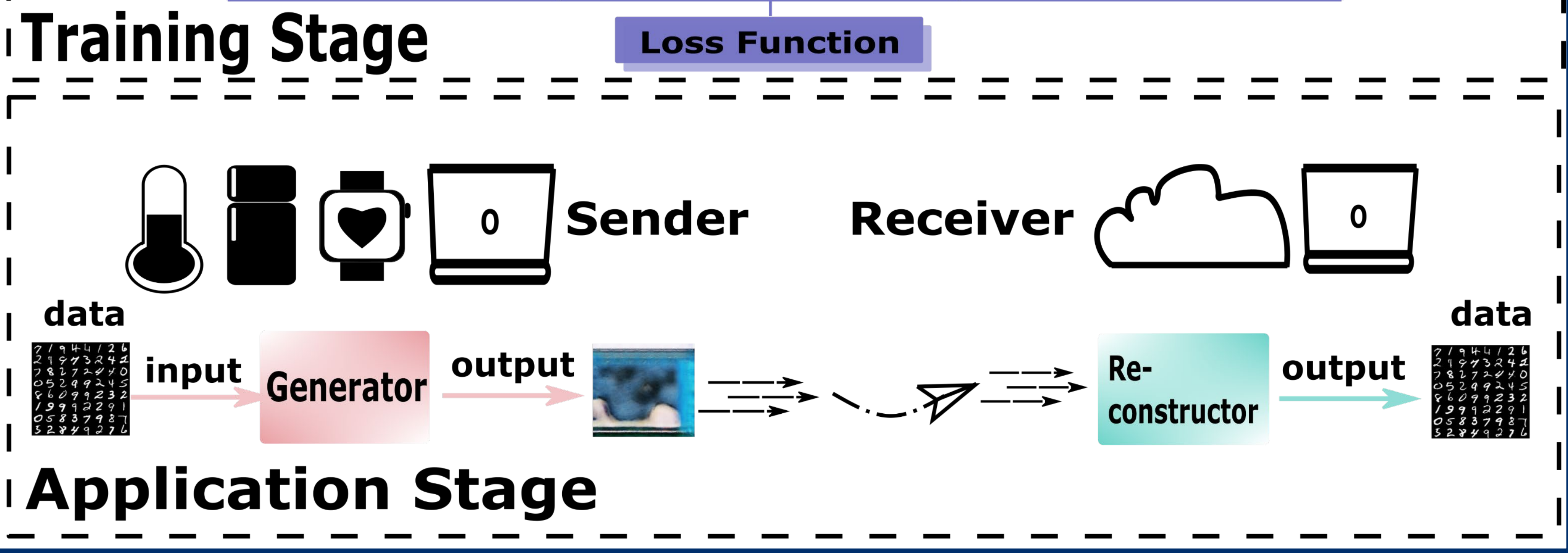## *Personalized gestures through motion transfer: Protecting Privacy in Pervasive Surveillance*[2]

3D Point Extraction

Motion Transfer

target motion

source motion

get frames from videos → moving area detection from frames → get segmentation from frames → posture normalization → shape-based 2D points generation

Decoder

PointGest

f_i PointNet++ LSTM LSTM a_t

f_{t+1} PointNet++ LSTM LSTM a_{t+1}

f_{t+15} PointNet++ LSTM LSTM a_{t+15} output

PointGest with Attention Mechanism

Encoder

FC FC FC

LC

FC FC

FC: Fully Connected Layer
LC: Loss Computation

GIHNET: Lightweight, Secure IoT Communication[3]

Image bank

recovered data

Reconstructor

input data START **Generator**

recovered img **Generator**

START random input from image bank **Reconstructor**

generated representation

generated representation

S. Adv. Classifier A   **Classifier A**   **Classifier B**   **S. Adv. Classifier B**

Training Stage

Loss Function

Smart devices in the environment

- Devices: smart thermometer
- Attack: data breach
- Solution: a lightweight, secure IoT communication through data encryption using GAN-based method.

Sender   **Receiver**

data input **Generator** output → **Re-constructor** output data

Application Stage

Aalto University

[1] Zuo, S. , Sigg, S. , Nguyen, L. , Beck, N. , Jähne-Raden, N. & Wolf, MC , 2 Dec. 2022, in: IEEE Access. 10 , pp. 128682-128696.

[2] Zuo, S. & Sigg, S. , 2022 , in: IEEE Pervasive Computing. 21 , 4 , pp. 8-16.

[3] Zuo, S. & Sigg, S. , in: IEEE Internet of Things, under review.