63rd FITCE International Congress

26 – 28 September 2024, Kraków, Poland

Privacy-preserving Framework for Automated Detection of Arrhythmias from ECG Data

Kacper Gil, Andres Vejar

Institute of Telecommunications

AGH University of Krakow, Kraków, Poland

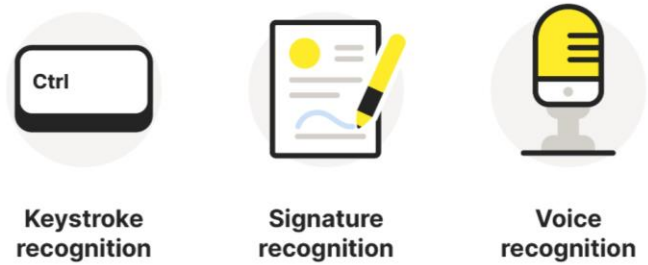
Outline

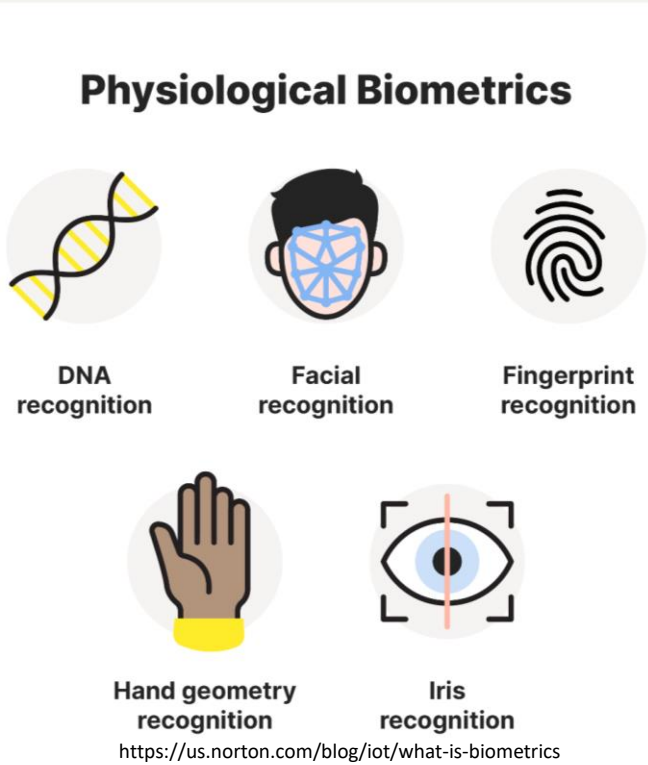
1. **Introduction**
   - Working principle
   - Biometric identification
2. **System Description**
3. **Results and Evaluation**
4. **Conclusion and Future Work**

Introduction

Automated diagnostic systems:

- Lower the workload of health facilities
- Contribute to the development of telemedicine
- Require biosignal tracking





https://us.norton.com/blog/iot/what-is-biometrics

Introduction (cont'd)

Considering the nature of the measured signals, it is crucial to provide a privacy centred approach. There are three types of privacy enhancing technologies (PETs), *see Jordan et al. (2022)* :

1. Algorithmic PETs:
   - homomorphic encryption
   - differential privacy
   - zero-knowledge proofs
2. Architectural PETs:
   - federated learning
   - multi-party computation
3. Augmentation PETs:
   - synthetic data
   - digital twinning

Sara Jordan, Clara Fontaine, and Rachele Hendricks-Sturrup. "Selecting Privacy-Enhancing Technologies for Managing Health Data Use". In: Frontiers in Public Health 10 (2022). DOI: 10 . 3389/fpubh.2022.814163.

Privacy approaches

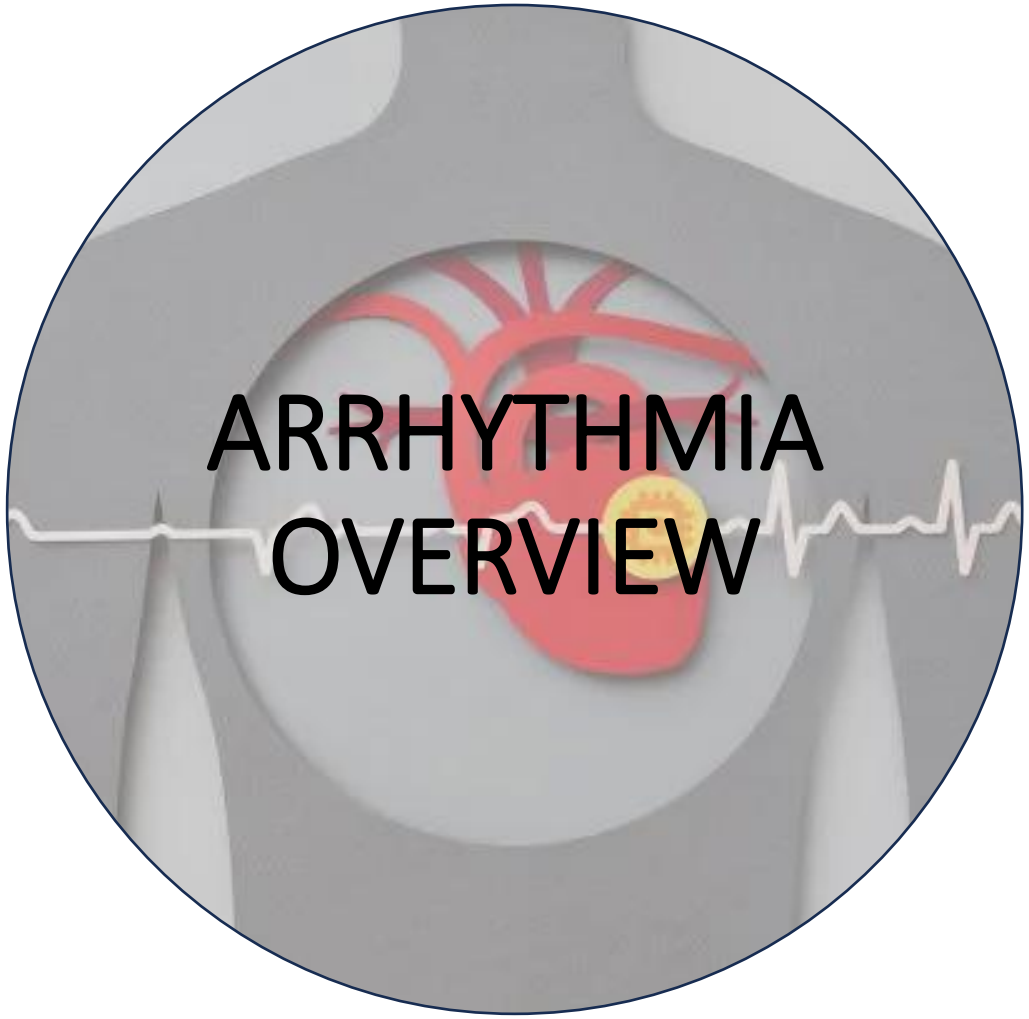
PETS - DEFINITION

Wide and varying definitions of privacy-enhancing technologies (PETs) persist in the research and practice of privacy engineering due, in part, to the multidisciplinary nature of the field.

PETs are described as encompassing everything from privacy policy languages to algorithmic forms of privacy protection, which unify “privacy-engineering methods,” “privacy-engineering techniques,” and “privacy-engineering tools,” and “privacy-by-design.”

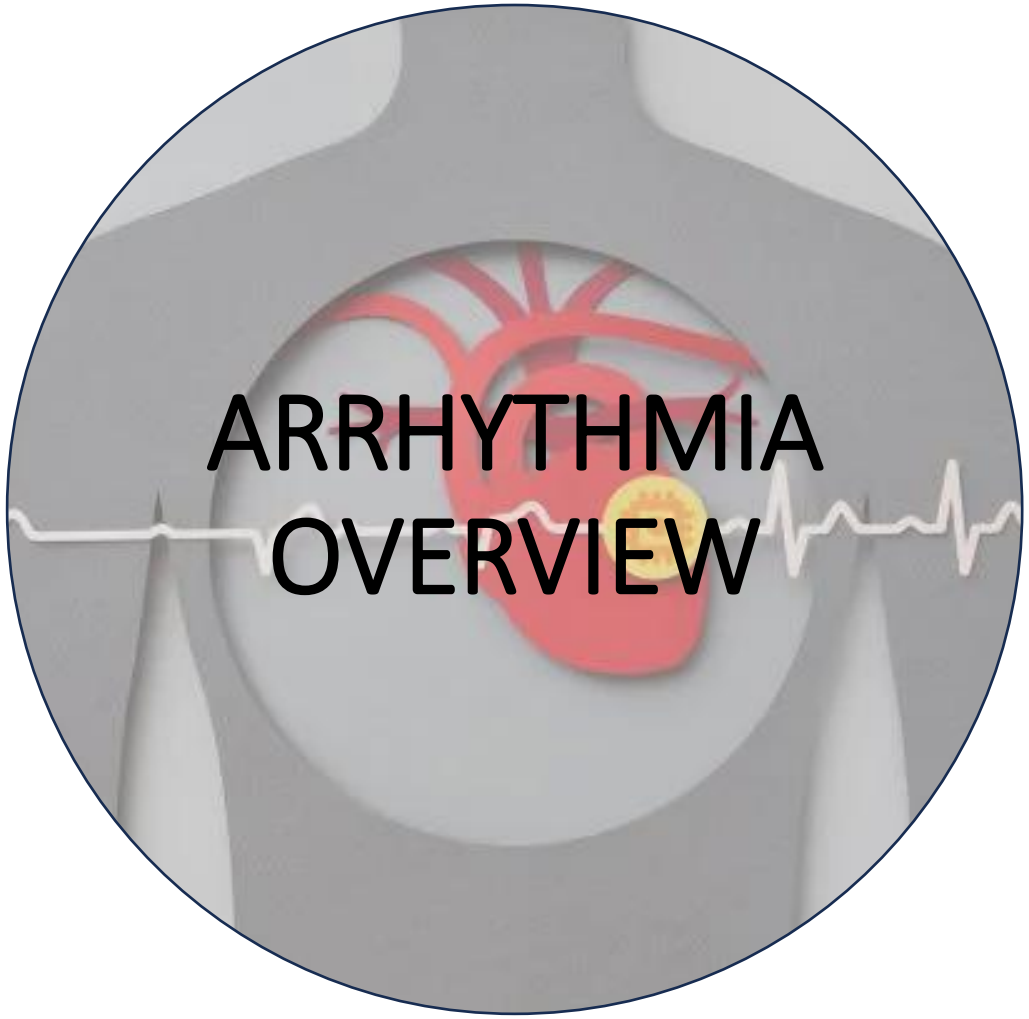
TYPES OF PETS

1. Algorithmic PETs:
   - homomorphic encryption
   - differential privacy
   - zero-knowledge proofs
2. Architectural PETs:
   - federated learning
   - multi-party computation
3. Augmentation PETs:
   - synthetic data
   - digital twinning



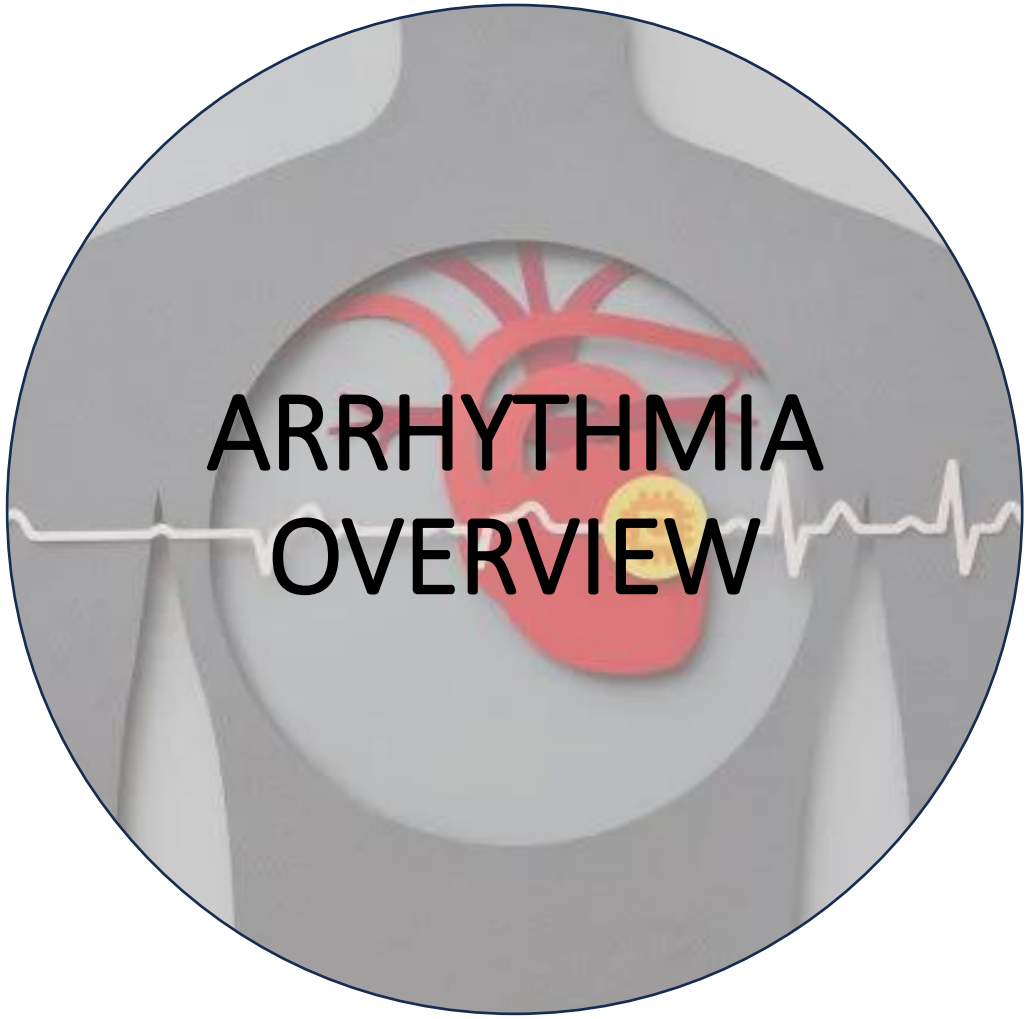
Characteristics of arrhythmia

Arrhythmia is a medical condition characterized by an irregular heartbeat, also classified as tachycardia or bradycardia if the heart beats too fast or too slow, respectively. Alternatively, the irregularity can display no pattern; in such cases it is called fibrillation.



Risk factors

- cardiovascular disease
- heart surgery
- cardiomyopathy
- electrolyte imbalances
- medication
- certain stimulants
- high levels of stress
- smoking
- physical exertion



Risk factors

- cardiovascular disease
- heart surgery
- cardiomyopathy
- electrolyte imbalances
- medication
- certain stimulants
- high levels of stress
- smoking
- physical exertion

Arrhythmia Detection System Privacy Preservation

- The research explores a machine learning diagnostic system for arrhythmia detection.
- Raw ECG biosignals undergo client-side pre-processing to create a filtered signal.
- The system aims to reduce discrepancies between preprocessed results and raw data classifier results, enhancing diagnostic precision and privacy.
- The application is tested with a non-privacy preserving control model to compare accuracy levels.
- Two stages of privacy enhanced ECG acquisition are considered: Feature Selection and Differential Privacy Transform.
- Feature Selection involves selecting useful temporal characteristics encoded into a signal.
- Differential Privacy Transform involves a controlled transformation to achieve differential privacy goals.

Biometric identification

Biometric Identification Phases

- Enrollment phase: Registers a source of biometric data with its associated identification index.
- Verification phase: Matches template data into new data.
- Enrollment phase can include diverse biometric data like fingerprints and face images.
- Verification phase can be challenging due to variation in biometric data.
- Biometric identification using ECG can be achieved directly or in conjunction with other sources of biometric data.

Biometric identification

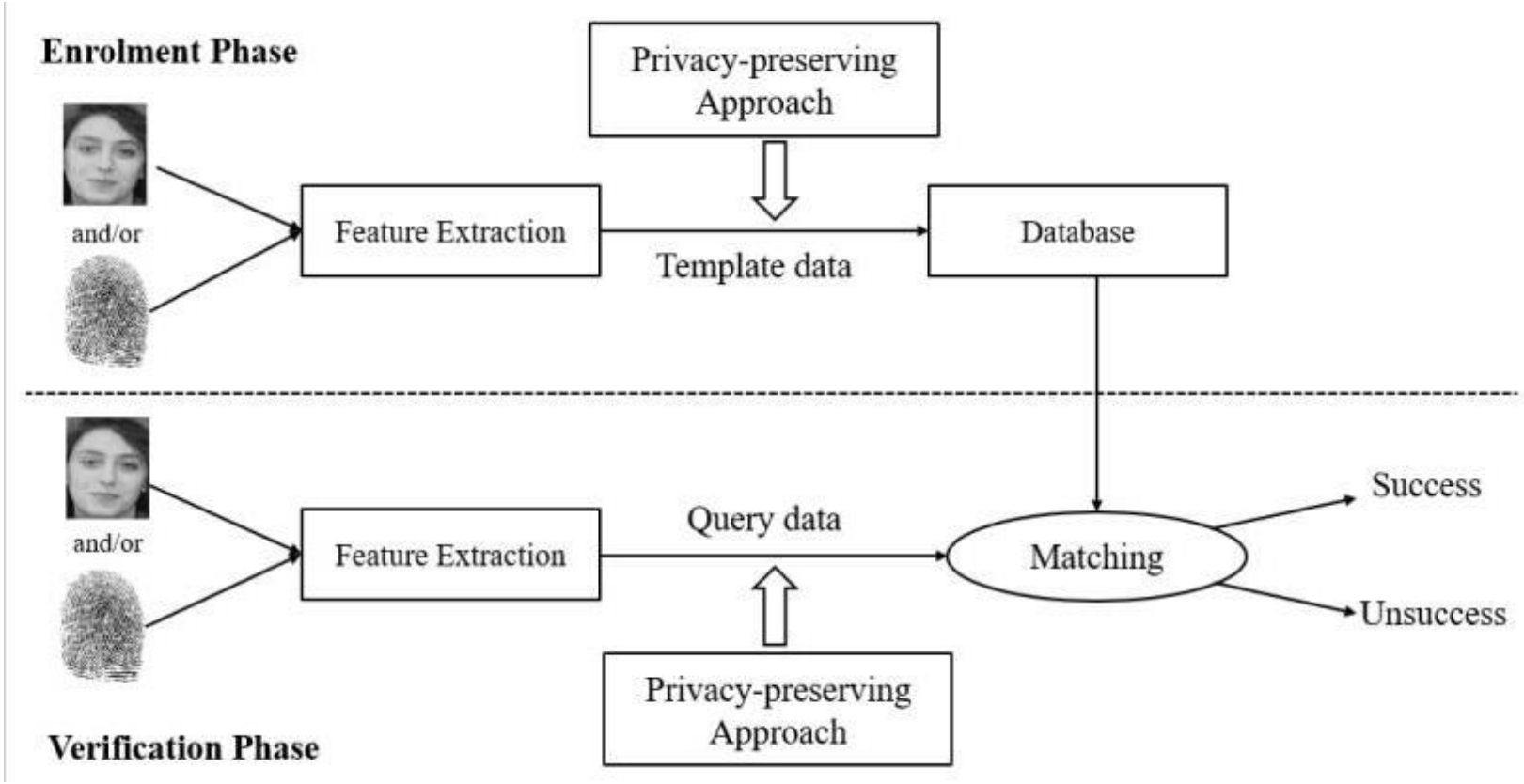


Figure 2: Biometric identification for a privacy-preserving system, from
Yang, W.; Wang, S.; Cui, H.; Tang, Z.; Li, Y. A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. *Sensors* **2023**, *23*, 3566. https://doi.org/10.3390/s23073566

.

Biometric identification

- Automated diagnostic systems reduce health facility load and improve home care quality.

- Tracking biosignals like EEG and ECG can reveal patient identities using biometric identification methods.

- Privacy should be built into technology, minimizing user data, controlling personal data, ensuring transparency, controlling authorized entities' data access, and securing data segregation.

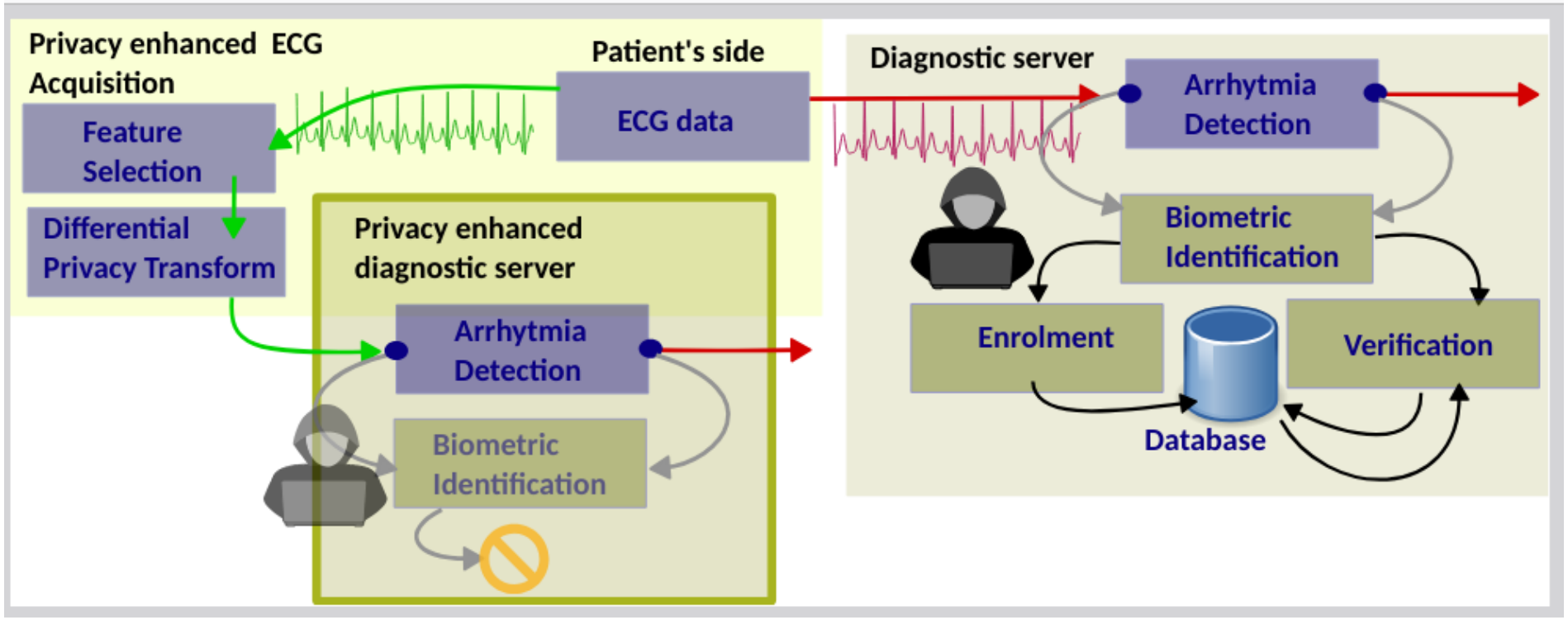
- Three categories of privacy-enhancing techniques (PET) exist: Algorithmic PETs, Architectural PETs, and Augmentation PETs.

- This work focuses on Algorithmic PET via differential privacy methods.

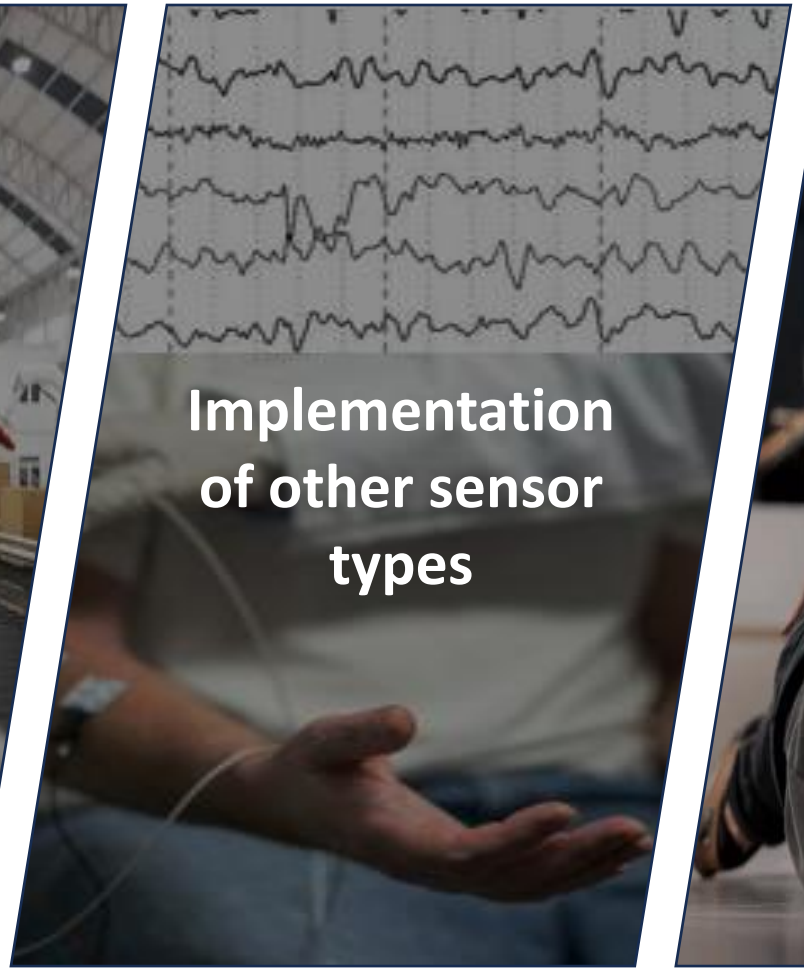
Privacy-Preserving Framework for Arrhytmia Detection

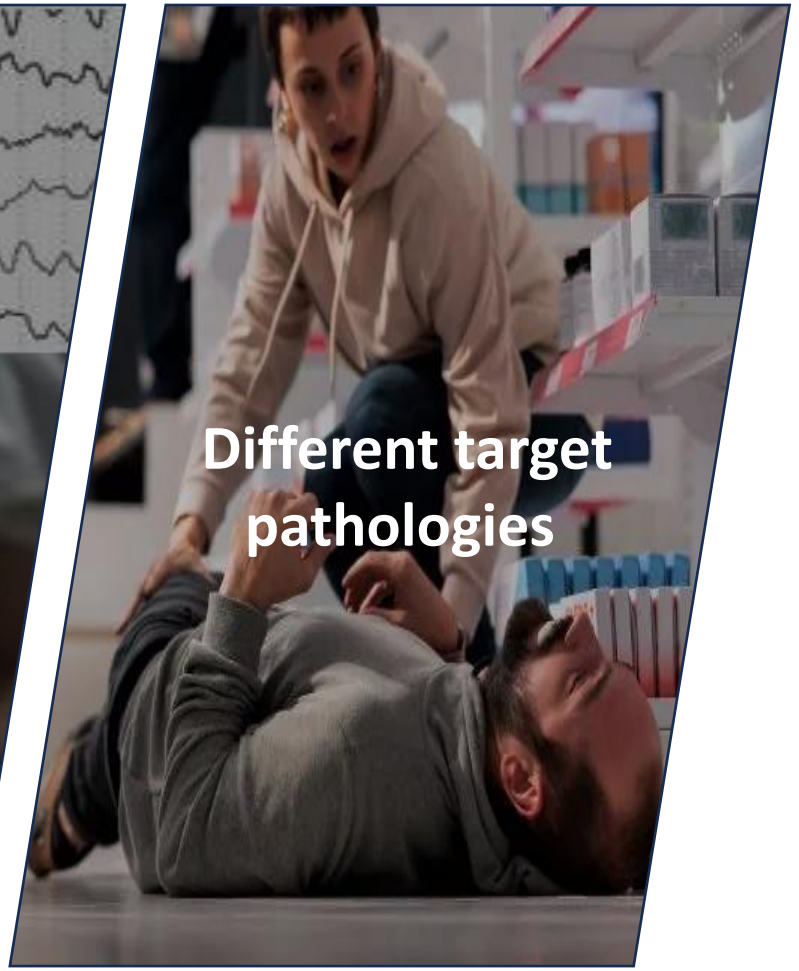
- Presents a privacy-preserving framework for remote diagnostic in homecare.
- Considers a 'Privacy enhanced ECG Acquisition' on the patient's side.
- A 'Privacy enhanced diagnostic server' provides automated diagnostic service.
- Ongoing work includes validation with standard ECG biosignal databases.
- Aims to promote privacy-enhancing technologies in early stages of automated diagnostic systems.
- Further work will explore design of automated diagnostic systems combining security and privacy.
- Expansion of approach includes use of various sensors and target pathologies.

Privacy-Preserving Framework for Arrhytmia Detection



Conclusions & Future Work





Conclusions & Future Work

- Importance of integrating machine learning for user data security and privacy.
- Exploration of anonymization and differential privacy frameworks to reduce biometric identification risk.
- Differential privacy method can used to filter biosignal data without compromising diagnostic trustworthiness.
- Proposed approach for privacy-preserving arrhythmia detection using machine learning.
- Evaluation can be done using control model to analyze accuracy difference with privacy-preserving input data.

Thank you for your attention!