Welcome to Biometric Security

(055047)

http://cse.hcmut.edu.vn/~khanh/teaching/BioSec2018/BioSec.html

Assoc. Prof. Dr. **DANG TRAN KHANH**

CSE/HCMUT, Vietnam

khanh@hcmut.edu.vn

Data SecuriTy Applied Research Lab

Course Introduction

BIOMETRIC SECURITY - 055047

Master Course of CS Programme (Sem2/2017-2018)

Lecture room: 215.B1, Sun (9:05-11:30)

Course structure:

Credit:	**3 (2.2.6)**		
Total Contact Hours:	**60**	Lectures: 45 Assignments: 15 Self-studying: 6 x 15 class hours	
Major	**Computer Science**		
Assessment:	Assignment	**10%**	Assign. presentation
		20%	Assign. report
	Presentation	**20%**	One time
	Final exam	**50%**	Open-book-exam (60')
	Bonus	added to "Final exam"	Additional presentation, exercises, etc.

Summary

This course provides knowledge about biometrics and its applications in computer security. In this course, biometric system architecture and various biometric systems based on fingerprints, face, iris and other modalities will be discussed. Biometric system performance and issues related to the security and privacy aspects of these systems, especially biometric template protection methods, will be addressed.

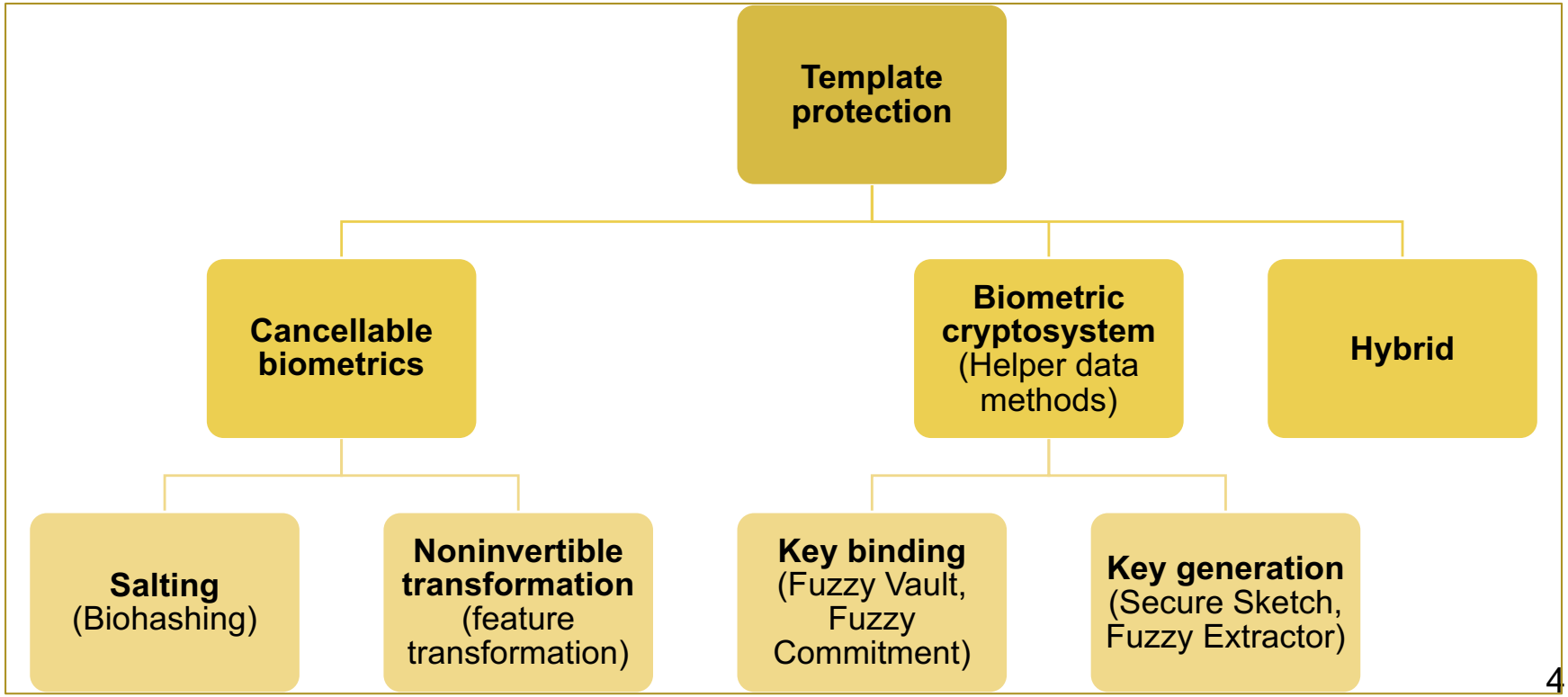
Biometric System Architecture and Security

Assoc. Prof. Dr. **DANG TRAN KHANH**
CSE/HCMUT, Vietnam
khanh@hcmut.edu.vn

Data SecuriTy Applied Research Lab

Contents (1 & 2 for today)

1. Biometrics: A Quick Introduction
2. Biometric System Architecture



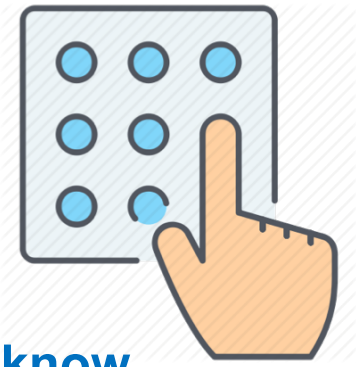
Contents

Part 1: Introduction about biometrics

- Introduction
- Biometric definition
- Biometric modalities
  - Physiological
  - Behavioral
  - Comparisons of various biometrics
- Comparing biometrics with token, password for authentication

Introduction

- Traditional authentication & cryptosystem:



Something you know

Something you have

- Biometrics: Something you are

Biometrics Definition (1)

- **Biometrics** (bio=life, metric=degree): the automatic recognition of individuals based on biological and behavioral traits

  (ISO/IEC JTC1/SC37 Standing Document 2: Harmonized Biometric Vocabulary)

- Requirements of a biometric characteristic:
  - **Universality**: each person should have the characteristic
  - **Uniqueness**: The characteristic of any two persons should be sufficiently different
  - **Permanence**: The characteristic of an individual should be sufficiently invariant over time

  (Anil K. Jain, Arun Ross, and Salil Prabhakar (2004): An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, 14:4-20*)*

Biometrics Definition (2)

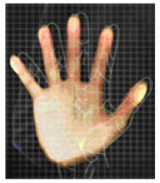
- Requirements of a biometric characteristic (cont.):
  - **Measurability**: The characteristic can be measured quantitatively
  - **Performance**: The characteristic can be achieved the desired recognition accuracy, speed, resource
  - **Acceptability**: People are willing to accept the use of a the characteristic in their daily lives
  - **Circumvention**: The characteristic is not able to be/ hardly faked using fraudulent methods

Biometrics Definition (3)

- Advantages of biometrics
  - Traditional approaches cannot differentiate between an authorized user and an impersonator
  - Uncomfortable: forgettable, lost,…
- Security and privacy concerns
  - Secure but not secret
  - Cannot be revoked or canceled
  - Once lost, forever compromised
  - Cross-matching

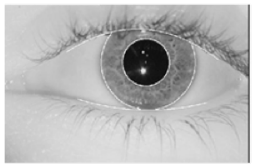
Biometrics modalities (1)

Fingerprint



Hand Geometry

Face



Iris

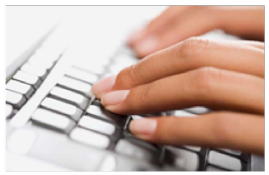
DNA

Physiological

Behavioral

Voice

Keystroke



Signature

Gait

Biometrics modalities (2)

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	HIGH	LOW	MEDIUM	HIGH	LOW	HIGH	LOW
Fingerprint	MEDIUM	HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH
Hand geometry	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	MEDIUM	MEDIUM
Keystrokes	LOW	LOW	LOW	MEDIUM	LOW	MEDIUM	MEDIUM
Hand veins	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH
Iris	HIGH	HIGH	HIGH	MEDIUM	HIGH	LOW	HIGH
Retinal scan	HIGH	HIGH	MEDIUM	LOW	HIGH	LOW	HIGH
Signature	LOW	LOW	LOW	HIGH	LOW	HIGH	LOW
Voice	MEDIUM	LOW	LOW	MEDIUM	LOW	HIGH	LOW
Facial thermograph	HIGH	HIGH	LOW	HIGH	MEDIUM	HIGH	HIGH
Odor	HIGH	HIGH	HIGH	LOW	LOW	MEDIUM	LOW
DNA	HIGH	HIGH	HIGH	LOW	HIGH	LOW	LOW
Gait	MEDIUM	LOW	LOW	HIGH	LOW	HIGH	MEDIUM
Ear Canal	MEDIUM	MEDIUM	HIGH	MEDIUM	MEDIUM	HIGH	MEDIUM

(Anil K. Jain, Arun Ross, and Salil Prabhakar (2004): An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, 14:4-20)

Biometrics vs Token and Password

	User Authentication		
	Knowledge-Based	Object-Based	ID-Based
Commonly Referred To as:	Password, Secret	Token	Biometrics
Support Authentication by:	Secrecy or obscurity	Possession	Uniqueness and personalization
Examples	Password, PIN	Key, ID card, member card	Fingerprint, Face, Iris
Copied	"Software"	Easy to very difficult	Easy to difficult
Lost	"Forgotten"	Easy	Very difficult
Stolen	Spied	Possible	Difficult

http://www.bromba.com/faq/biofaqe.htm

Biometrics vs Token and Password

Authenticator Combination	Security Advantage	Convenience Drawback	Example
Knowledge- and Object-Based	Lost/stolen token protected by password	Must carry token and memorize password	PIN-enabled bank card
Object- and ID-Based	Lost/stolen token protected by ID	Must carry token, but not ID if it is a biometric	Photo-ID
Knowledge- and ID-Based	Two factors provide security in case either compromised	Have to memorize password and have ID.	Password and biometric for computer access.
Knowledge-, Object-, and ID-Based	A third factor to provide security in case two other factors are compromised	Have to memorize password, carry token, and have ID.	Military applications requiring photo-ID checked by guard, plus password.

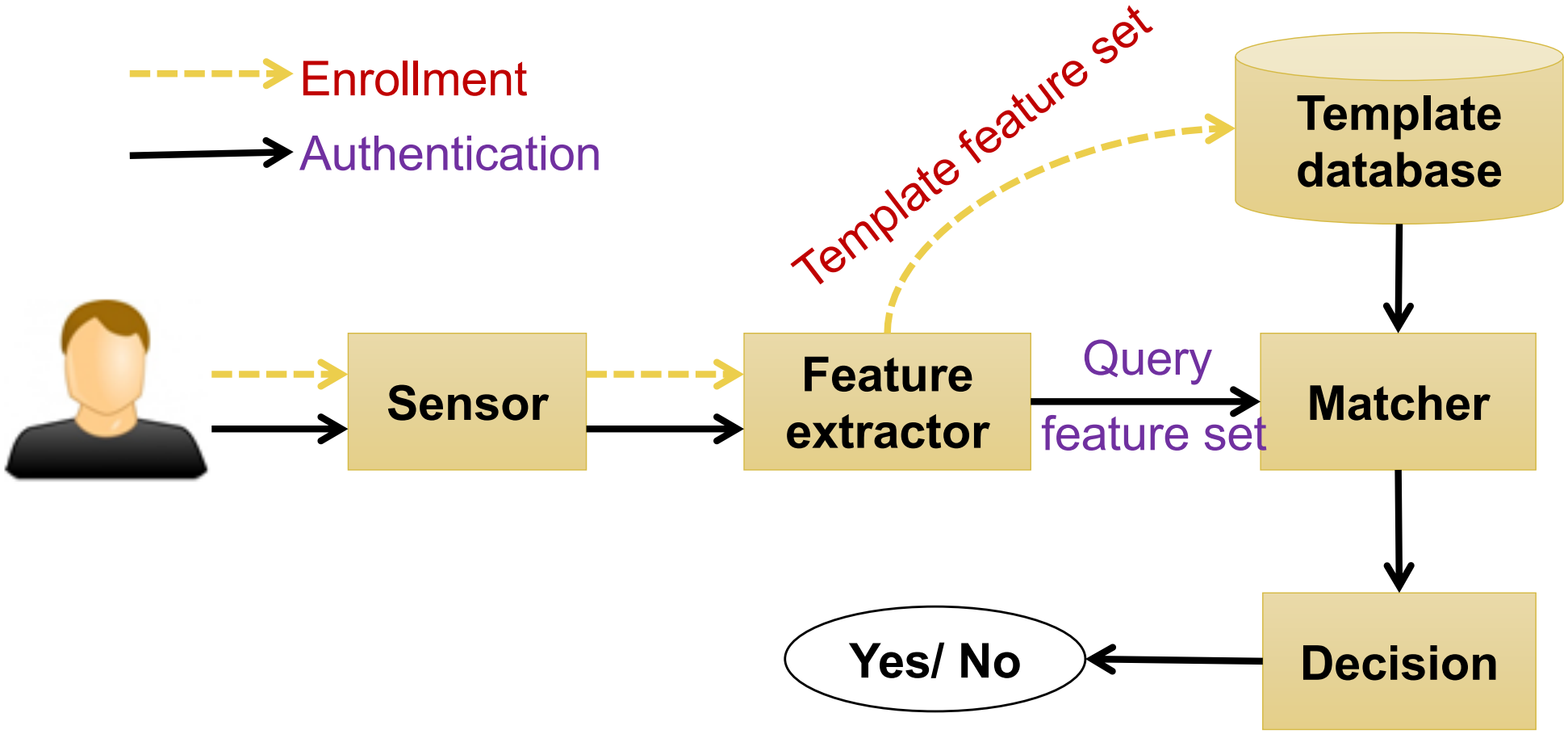
Security and Convenience of Combining authenticators

O'Gorman, Lawrence (2003): Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE,* 91(12): 2021-2040.

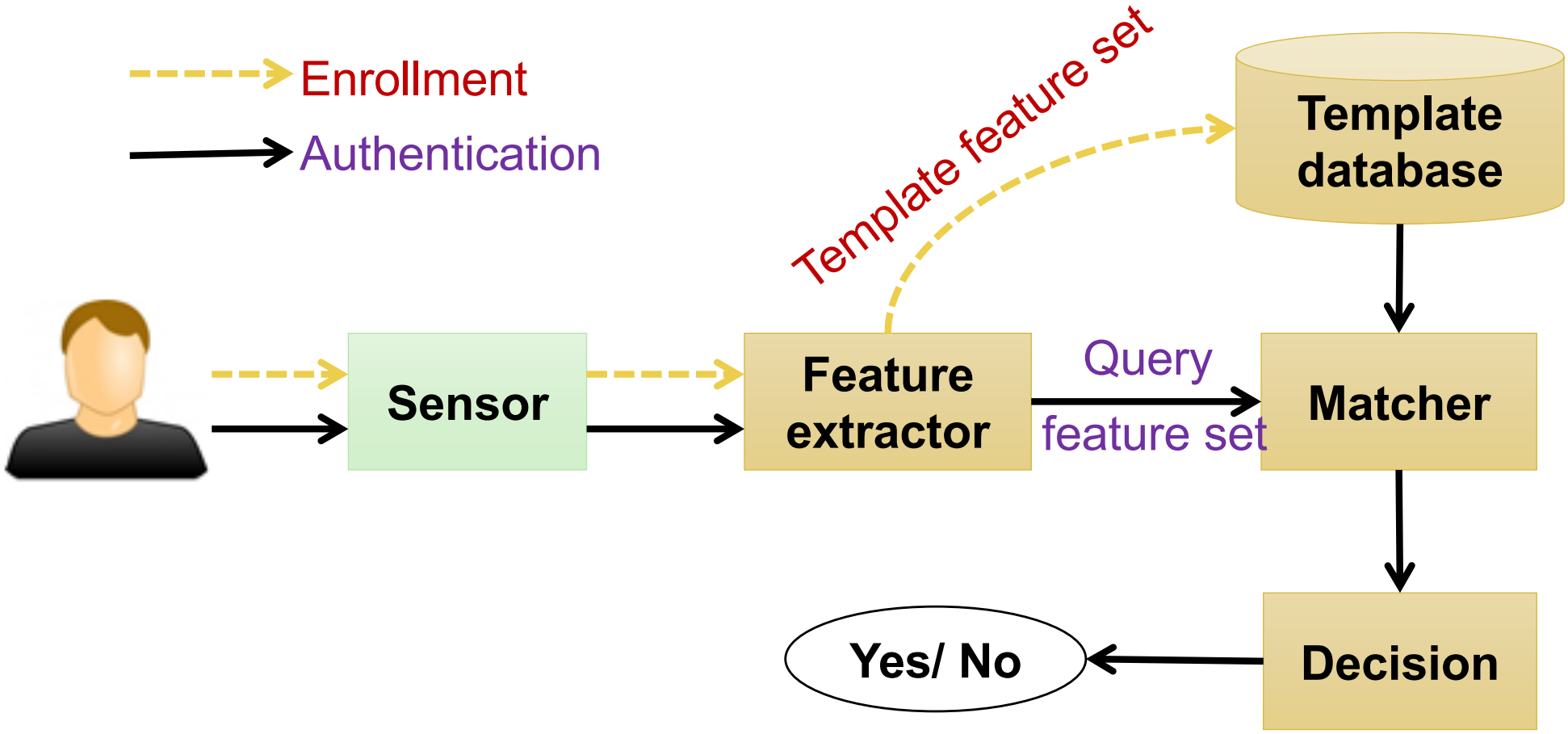
Part 2: Biometric System Architecture

- Biometric Authentication System
- Biometric Cryptosystem
- Biometric System Failures
- Attacks on the Biometric System

Biometric Authentication System

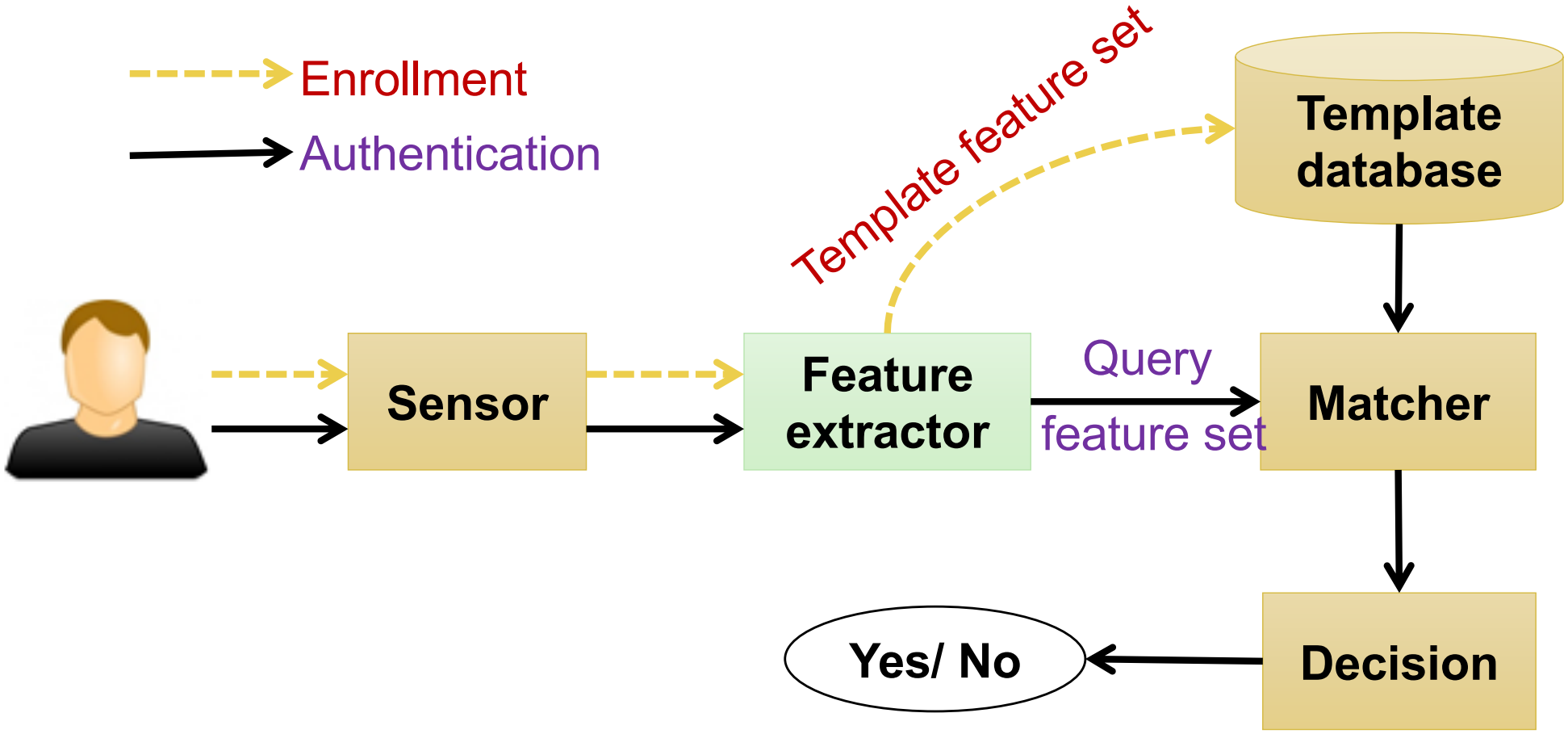


Biometric Authentication System



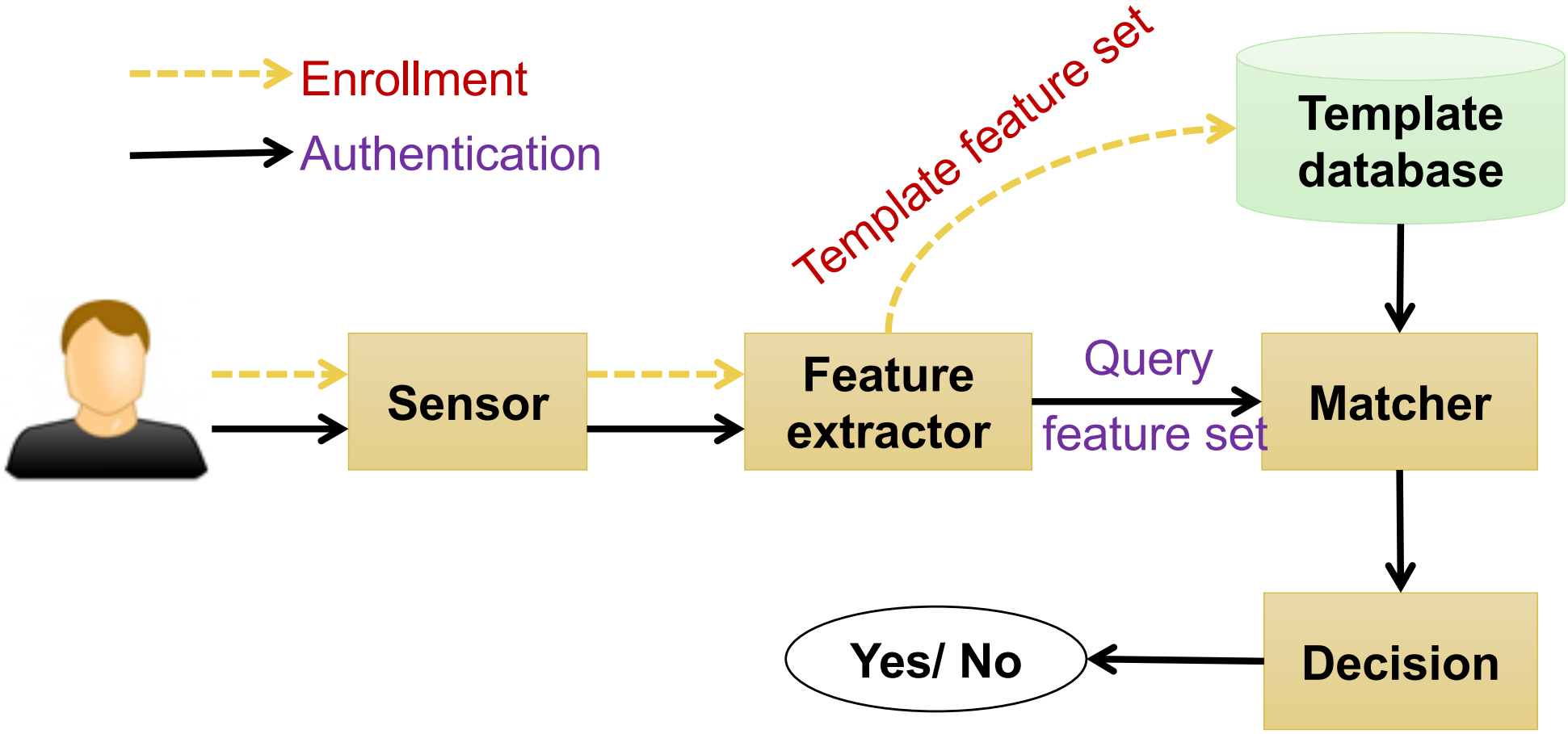
Sensor module: collects biometric trails from users

Biometric Authentication System



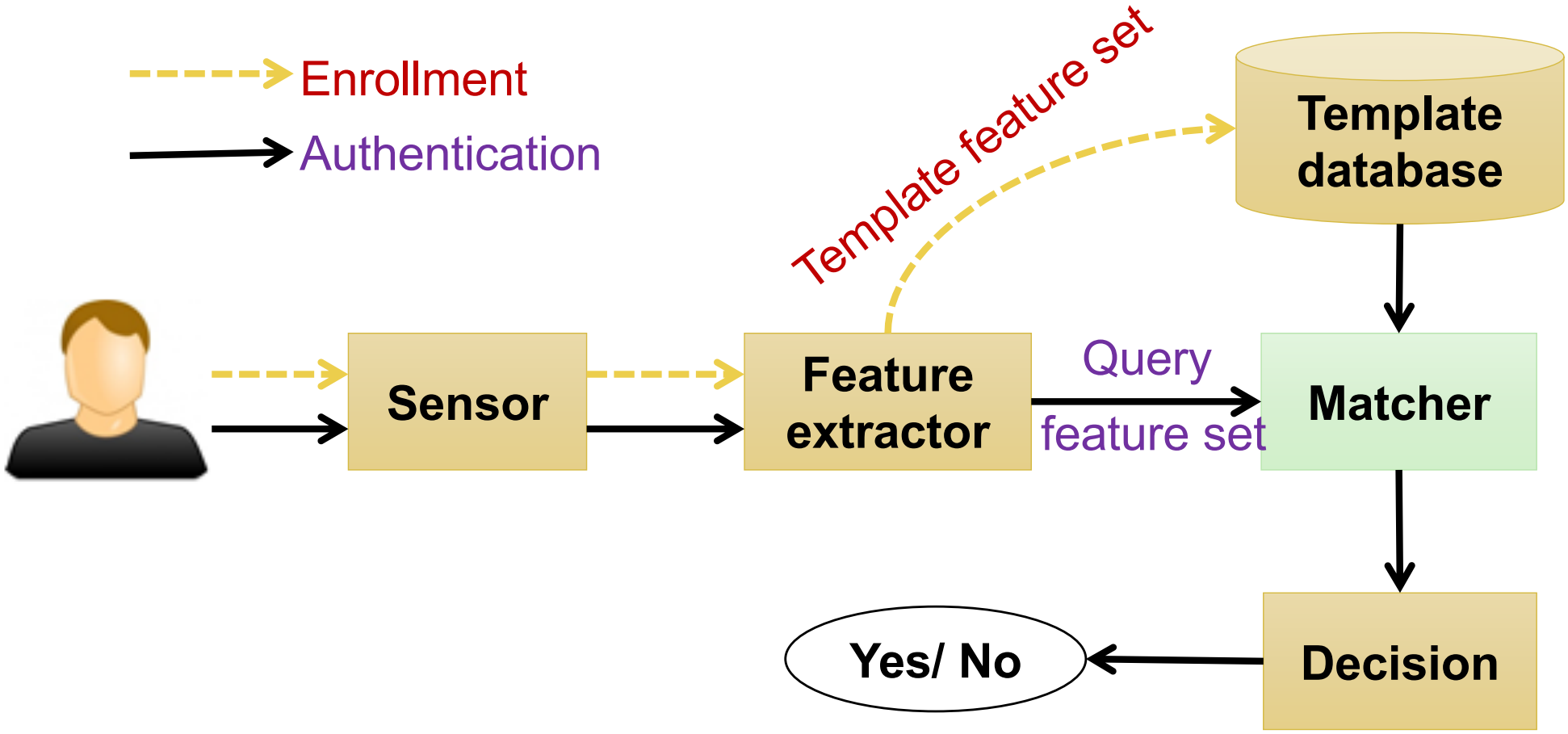
Feature extractor module: gets the biometric trails as raw data (images or signals) and extracts feature sets (template)

Biometric Authentication System



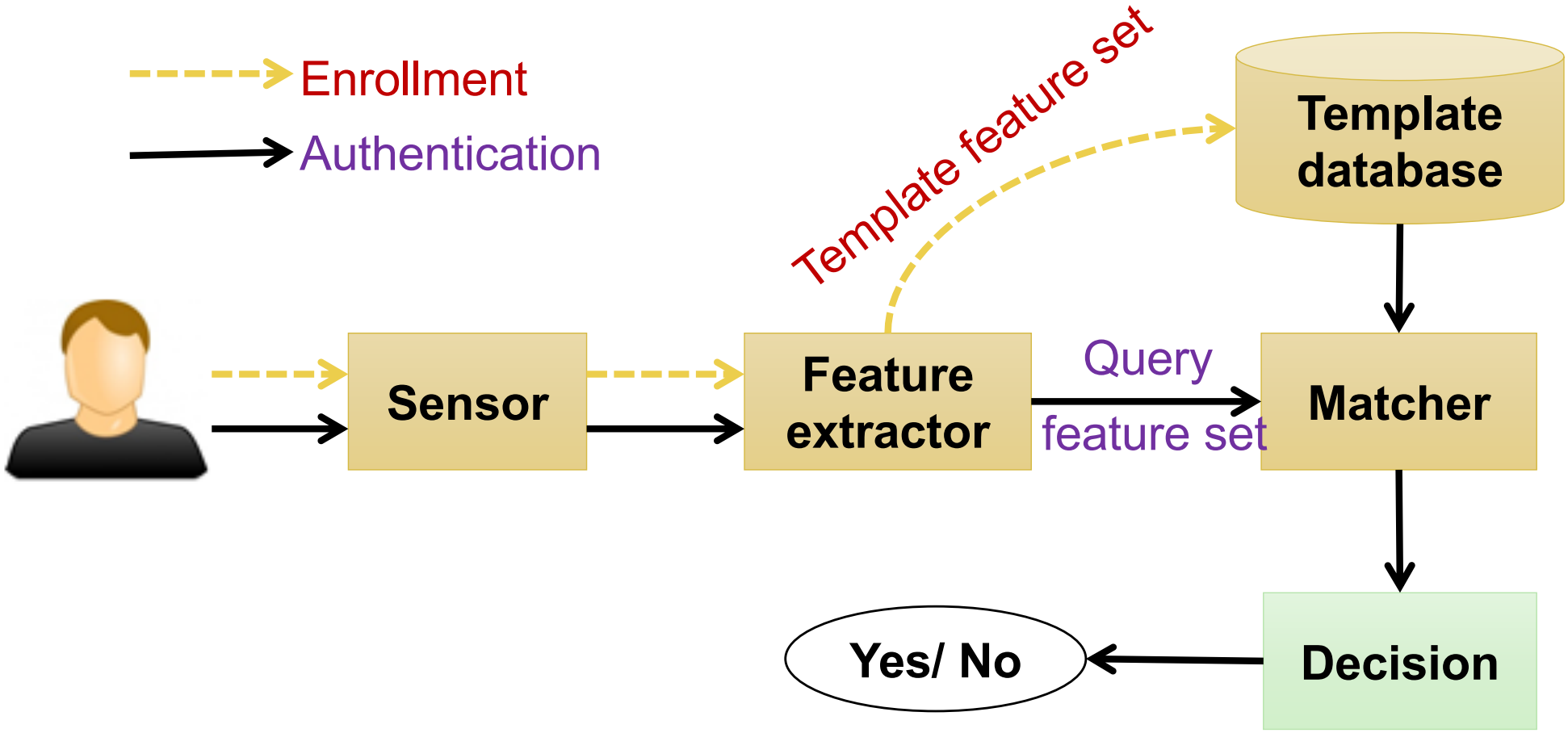
Template database: stores the extracted feature sets as templates

Biometric Authentication System



Matcher module: compares between template feature set and query feature set to compute a match score

Biometric Authentication System

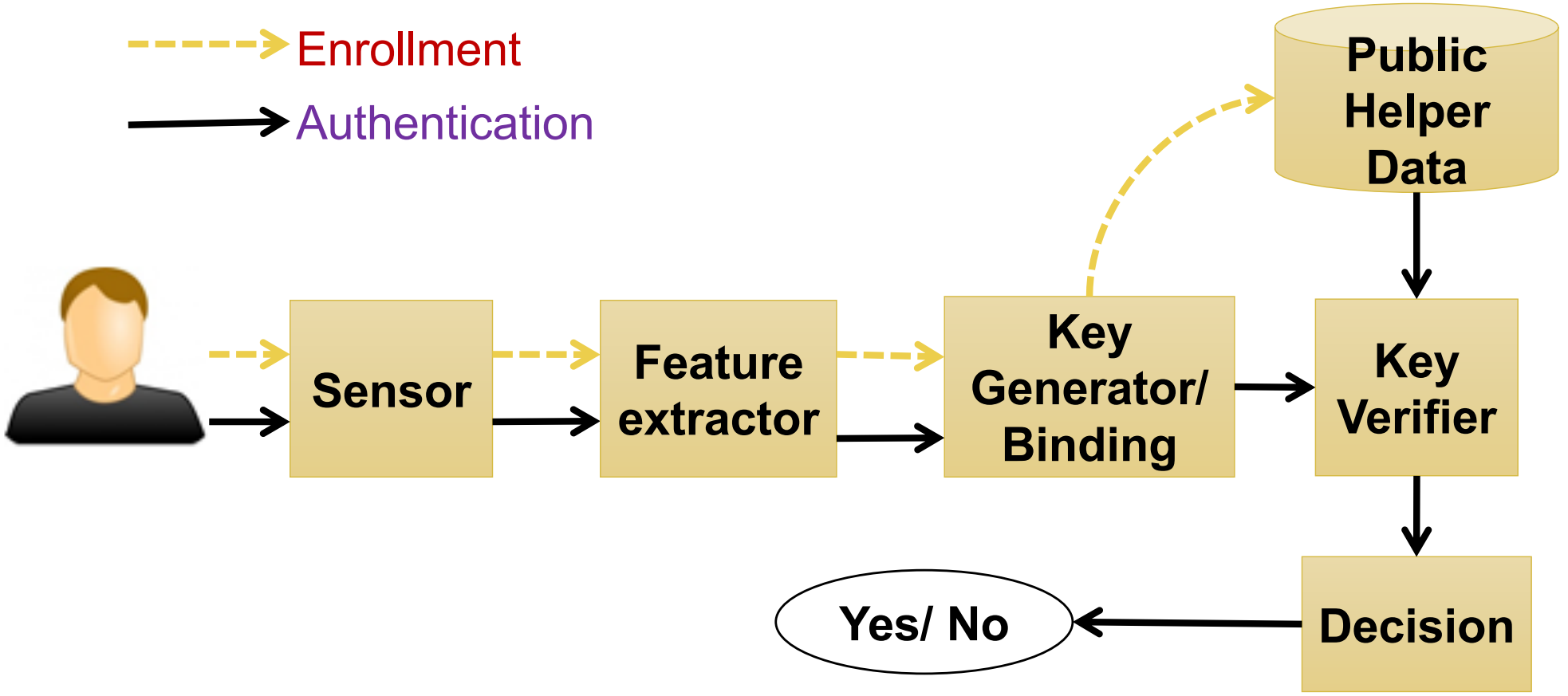


Decision module: gives a response (pass or fail to the authentication) based on the match score and a threshold

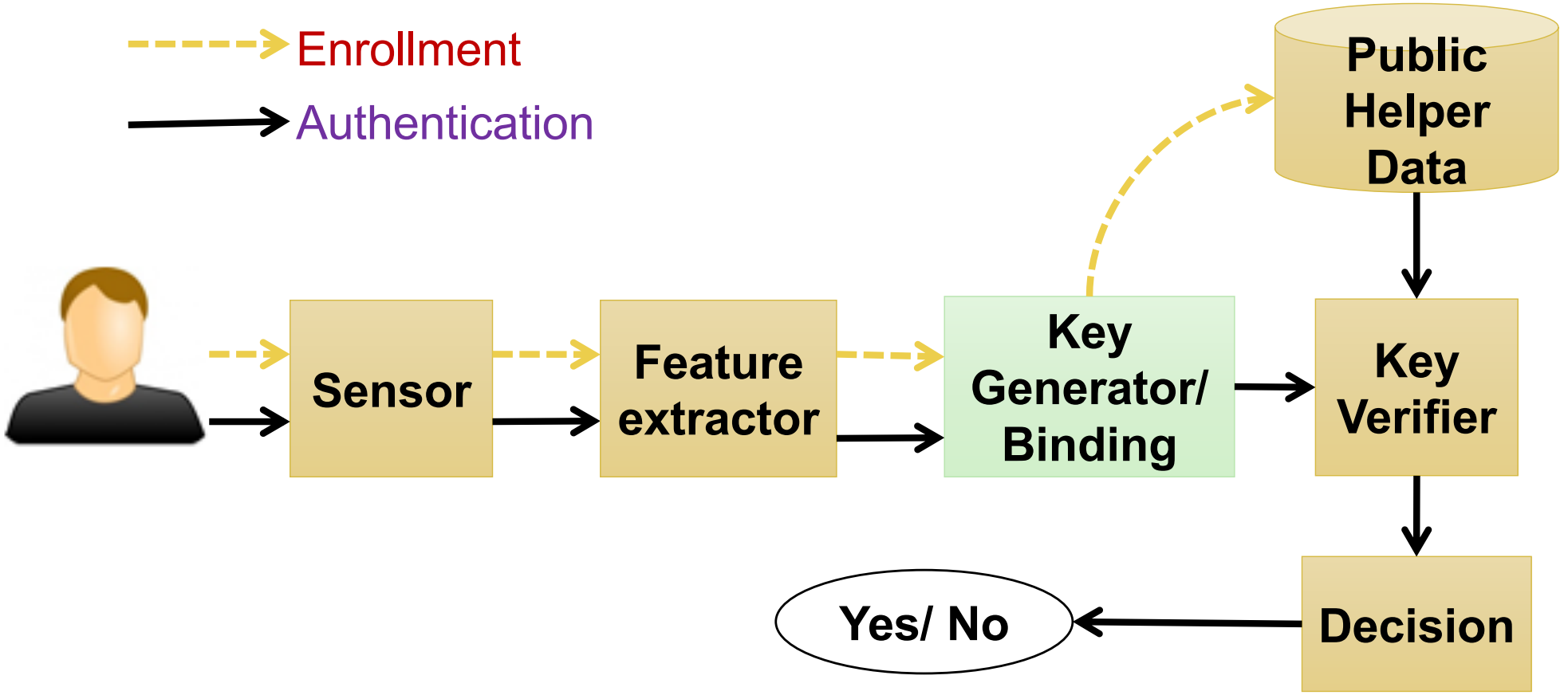
Part 2: Biometric System Architecture

- Biometric Authentication System
- Biometric Cryptosystem
- Biometric System Failures
- Attacks on the Biometric System

Biometric Cryptosystem

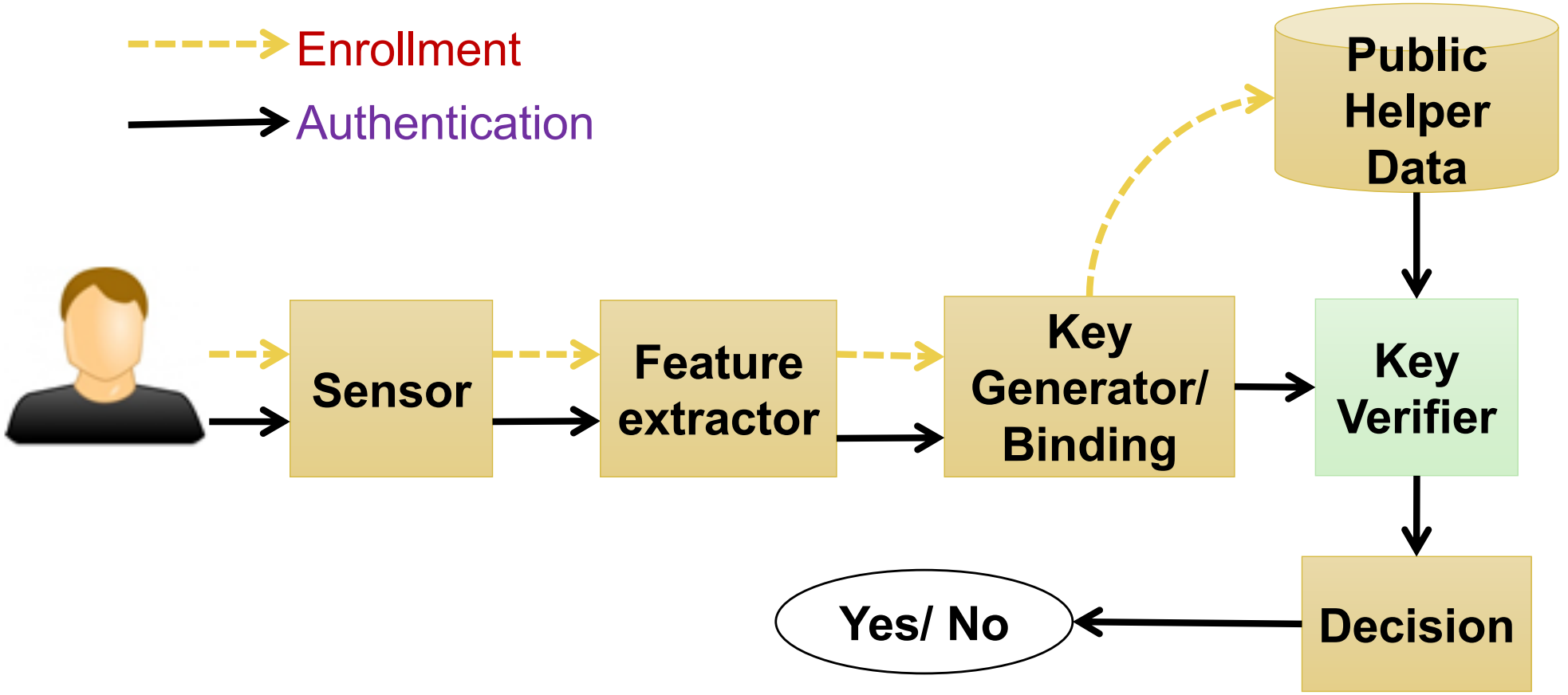


Biometric Cryptosystem



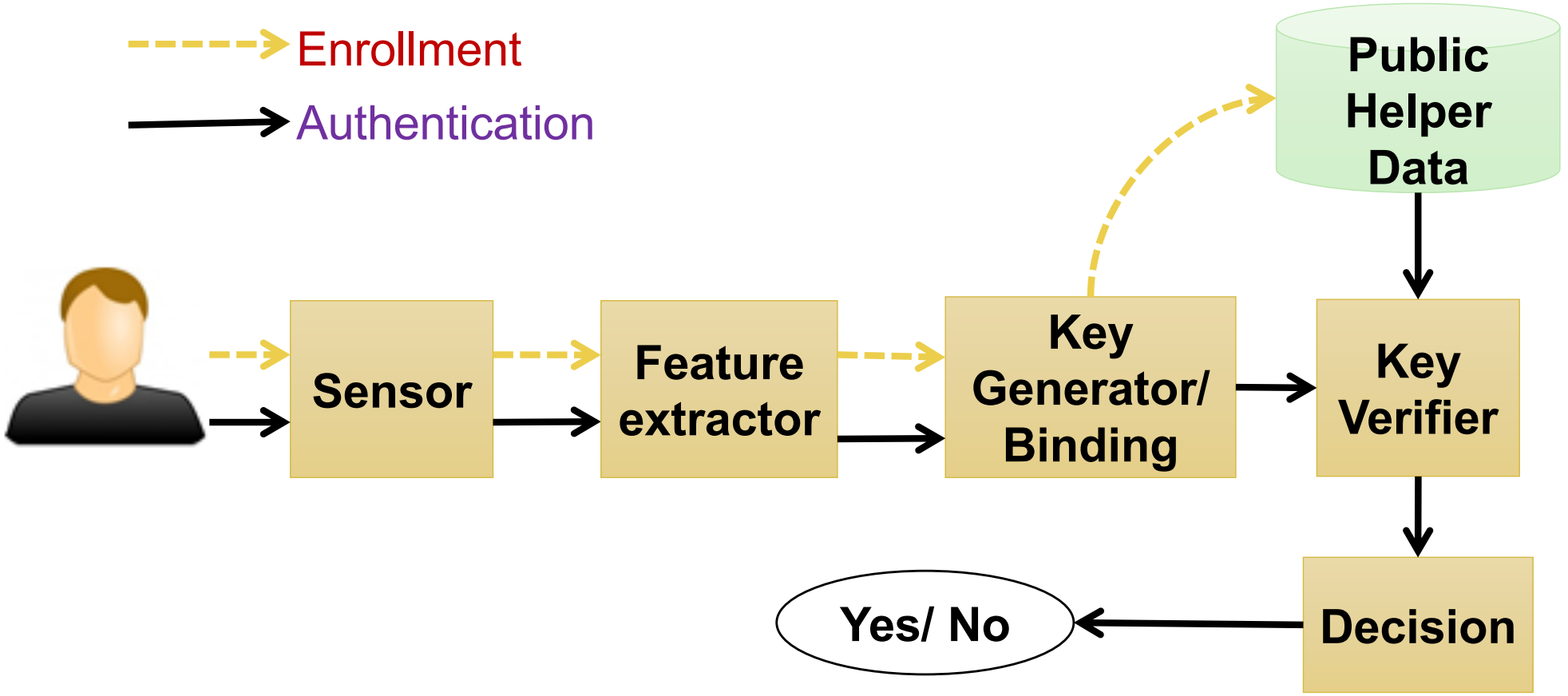
Key generator/ Key binding module: generating a key from the feature set or binding a key with the feature set

Biometric Cryptosystem



Key verifier: regenerates the key from the query feature set and public helper data

Biometric Cryptosystem

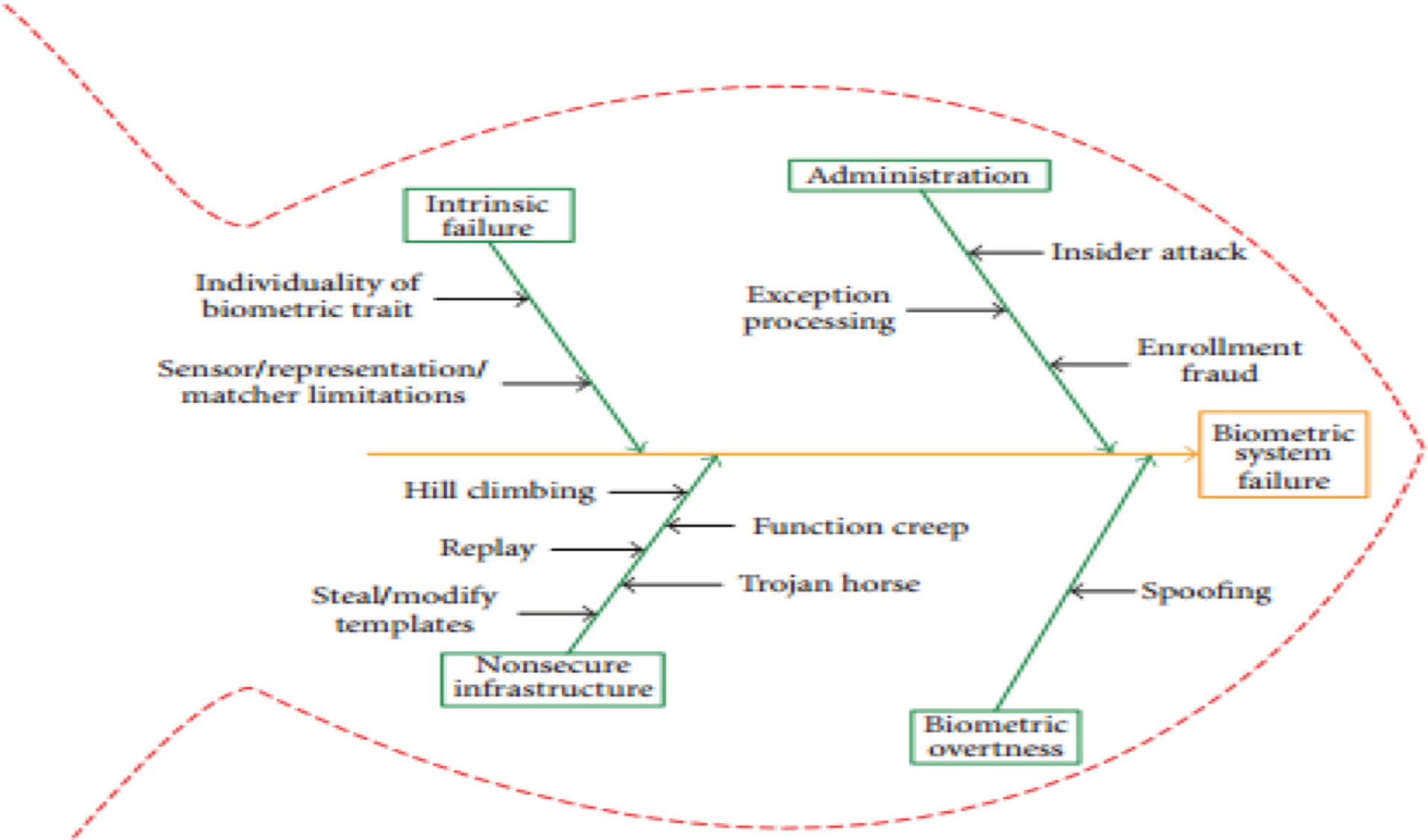


Public helper data: kind of public information about the biometric template. It is used to recover the key in the authentication process

Part 2: Biometric System Architecture

- Biometric Authentication System
- Biometric Cryptosystem
- Biometric System Failures
- Attacks on the Biometric System

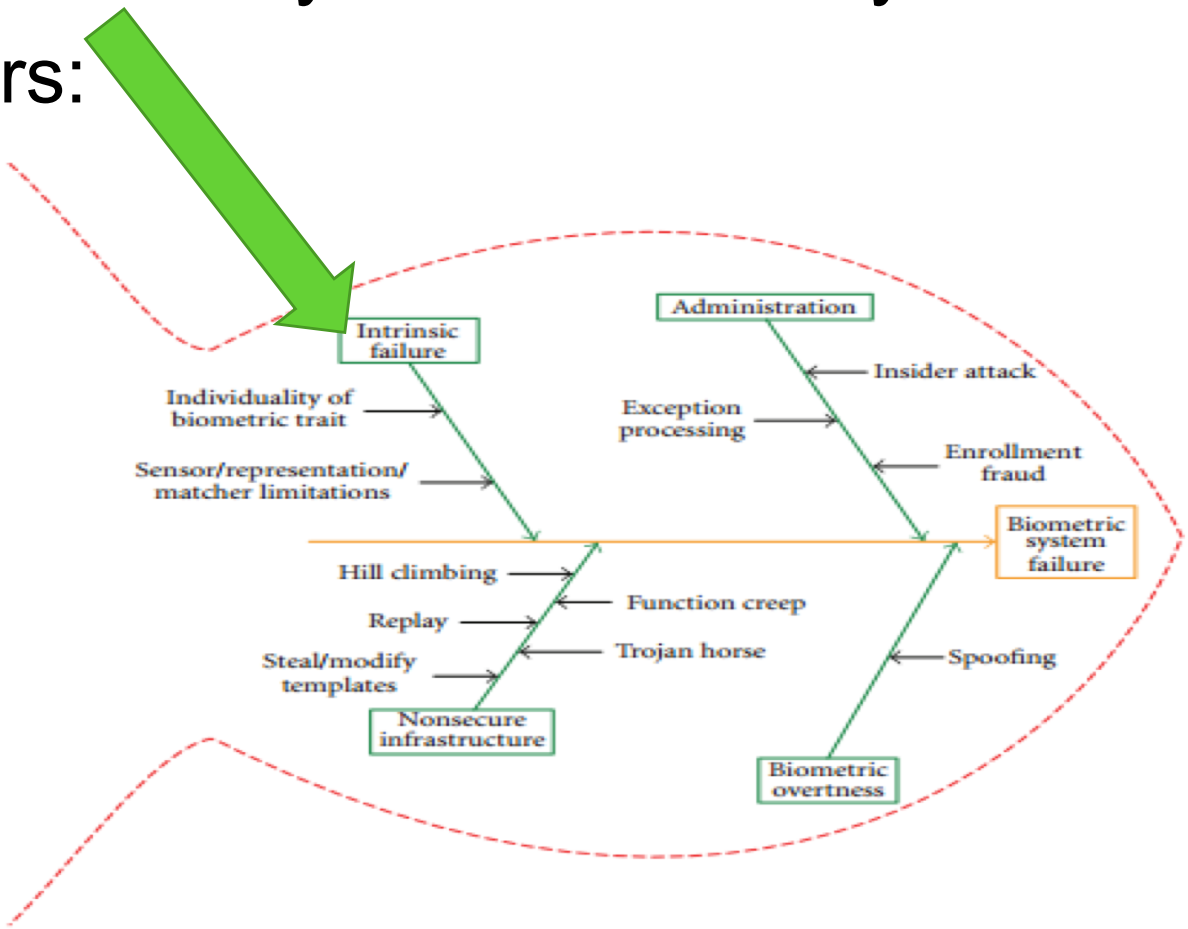
Biometric System Failures



Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar (2008): Biometric template security. *EURASIP Journal on advances in signal processing (article No. 113)*

Biometric System Failures

- **Intrinsic failure** is the security lapse due to an incorrect decision made by the biometric system
- Two types of errors:
  - False accept
  - False reject



Biometric System Failures

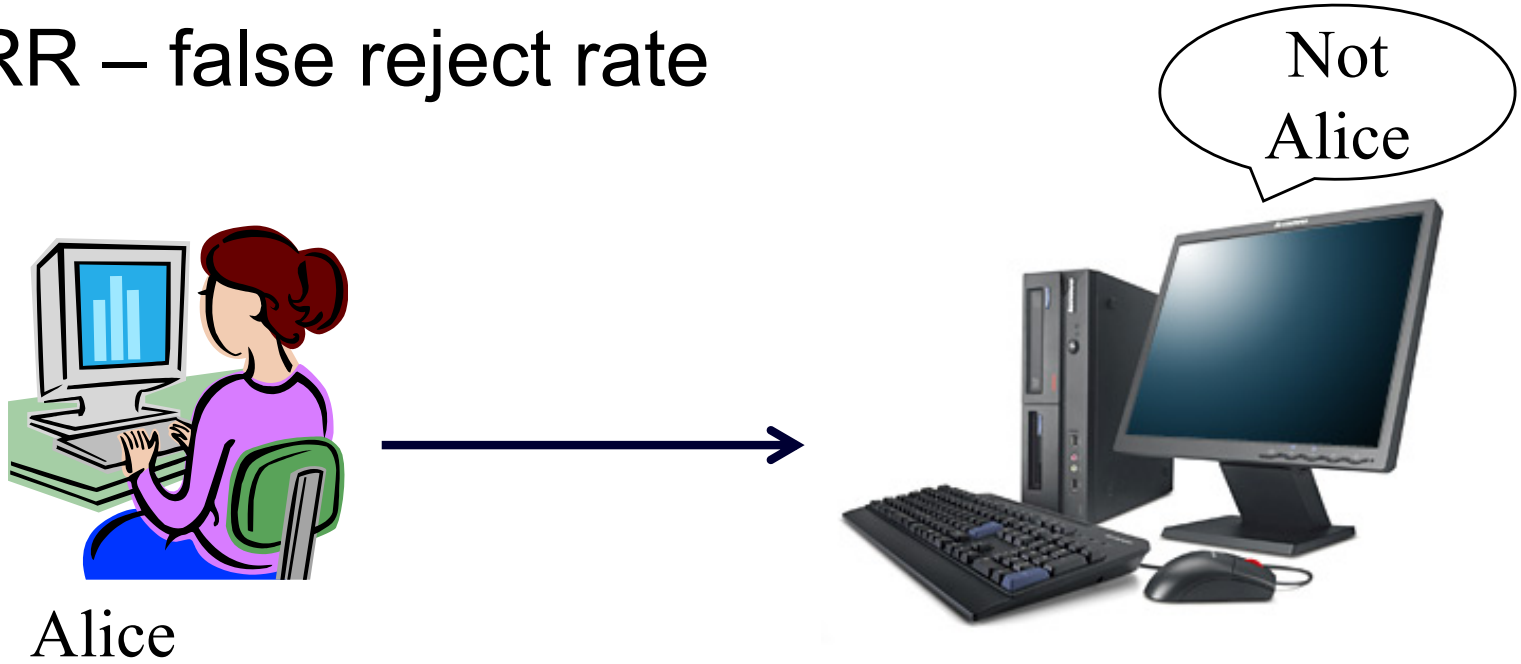
- **False accept:**
  - Intra-user similarity: Lack of individuality or uniqueness in the biometric trait which can lead to large similarity between feature sets of different users
- FAR - false accept rate

Bob

Biometric System Failures

- **False reject:**
  - Intra-user variations: due to incorrect interaction by the user with the biometric or the noise introduced at the sensor

- FRR – false reject rate



Biometric System Failures

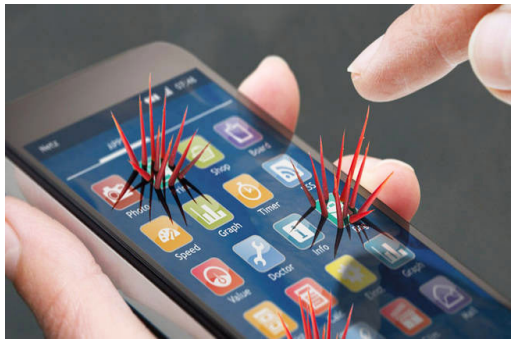
- **Intrinsic failures** can occur even when there is no explicit effort by an adversary to circumvent the system. So this type of failure is also known as **zero-effort attack**
- Reducing the probability of intrinsic failure through
  - New sensors: acquire the biometric traits of an individual in a more reliable, convenient, and secure manner
  - Development of invariant representation schemes, robust and efficient matching algorithms
  - Multi-biometric systems

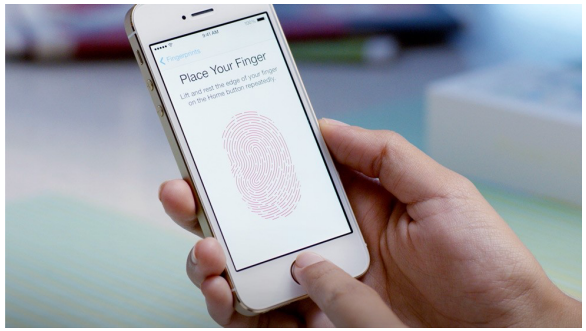
Biometric System Failures

- **Adversary attacks:** an adversary intentionally attack to the biometric system
- Three main classes:
  - Administration attack: due to improper administration of the biometric system (insider attack)
  - Non-secure infrastructure: hardware, software, and the communication channels
  - Biometric overtness: not distinguish between a live biometric presentation and an artificial spoof

Effects of biometric system failure

- When a biometric system is compromised, it can lead to two main effects
  - Denial-of-service: a legitimate user is prevented from obtaining the service that he is entitled to
    - Sabotage the infrastructure
    - Modification of templates or the operating parameters (e.g., matching threshold)
  - Intrusion
    - Unauthorized access to personal information



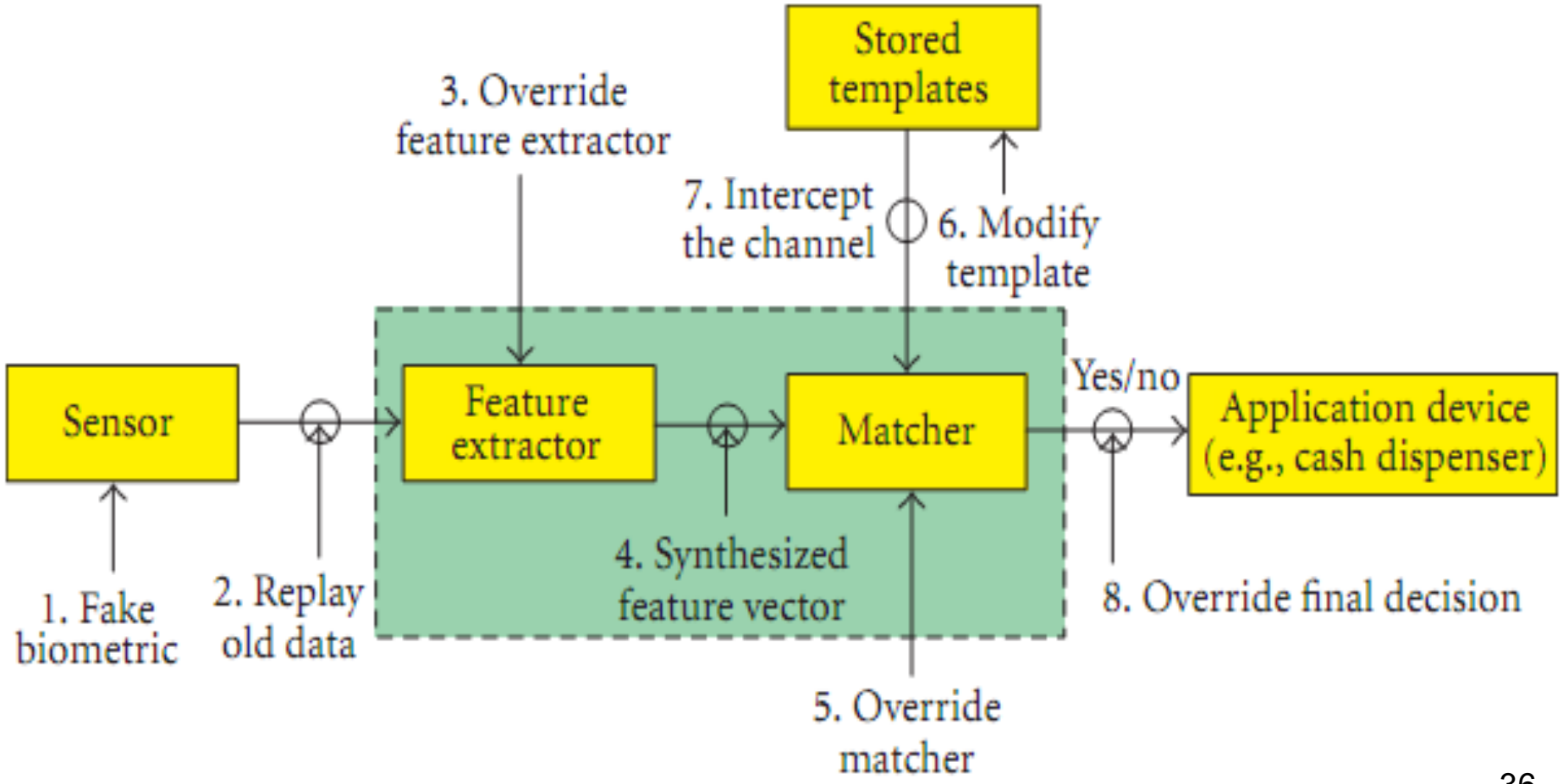


Part 2: Biometric System Architecture

- Biometric Authentication System
- Biometric Cryptosystem
- Biometric System Failures
- Attacks on the Biometric System

Countering adversary attacks

- Adversary attacks generally exploit the system vulnerabilities at one or more modules or interfaces



Countering adversary attacks

- Attacks at the user interface
- Attacks at the interface between modules
- Attacks on the software modules
- Attacks on the template database

Countering adversary attacks

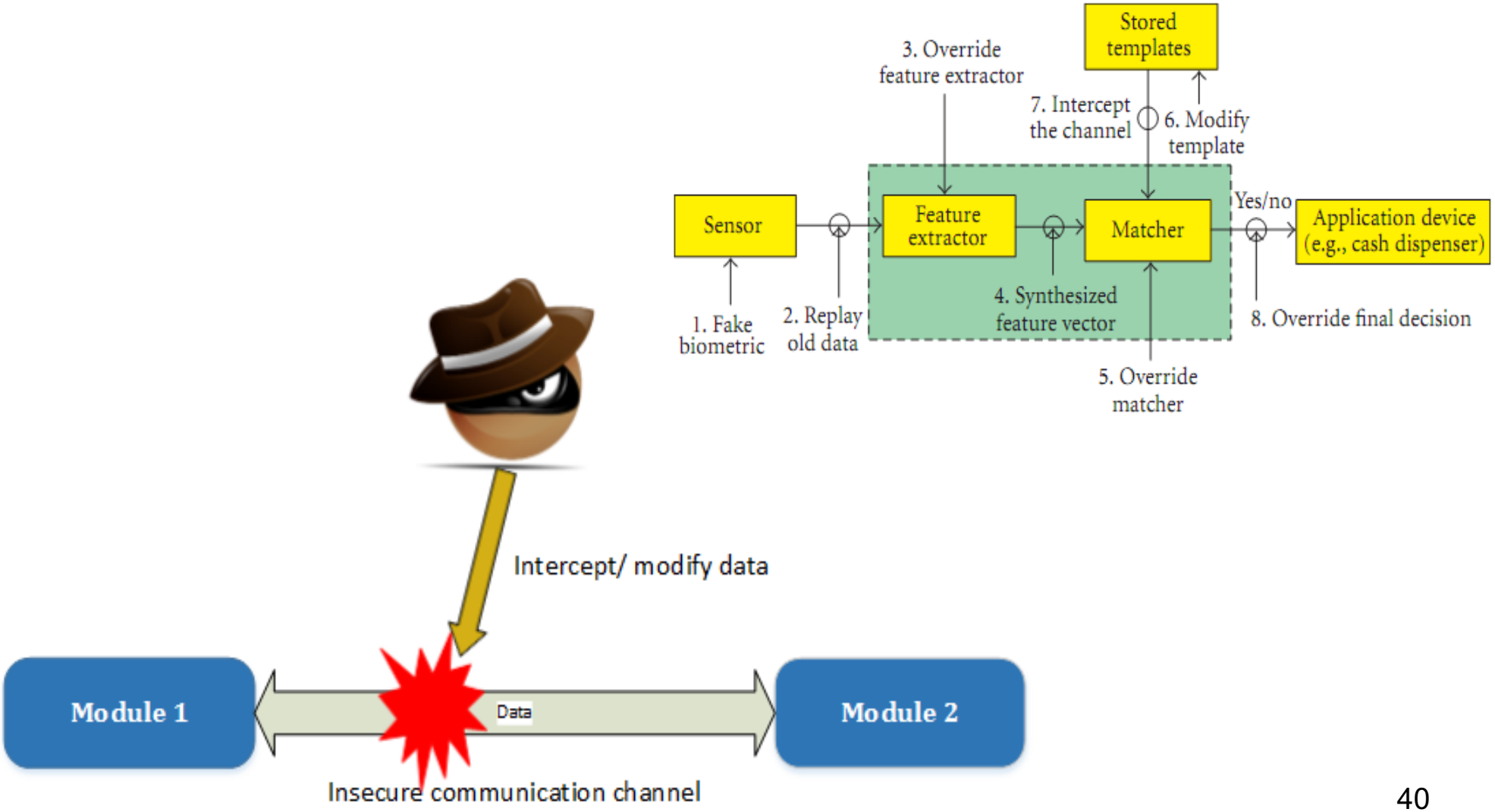
- **Attacks at the user interface:**
  - The sensor is unable to distinguish between fake and genuine biometric traits
  - Countermeasure: develop hardware as well as software solutions that are capable of performing liveness detection

Countering adversary attacks

- **Attacks at the interface between modules:**
  - Sabotage or intrude on the communication interfaces between different modules
  - If the channel is not secured physically or cryptographically, an adversary may also intercept and/or modify the data being transferred
  - Countermeasure: secure a channel by cryptography combining with time-stamps or a challenge/ response mechanism

Countering adversary attacks

- **Attacks at the interface between modules:**



Countering adversary attacks

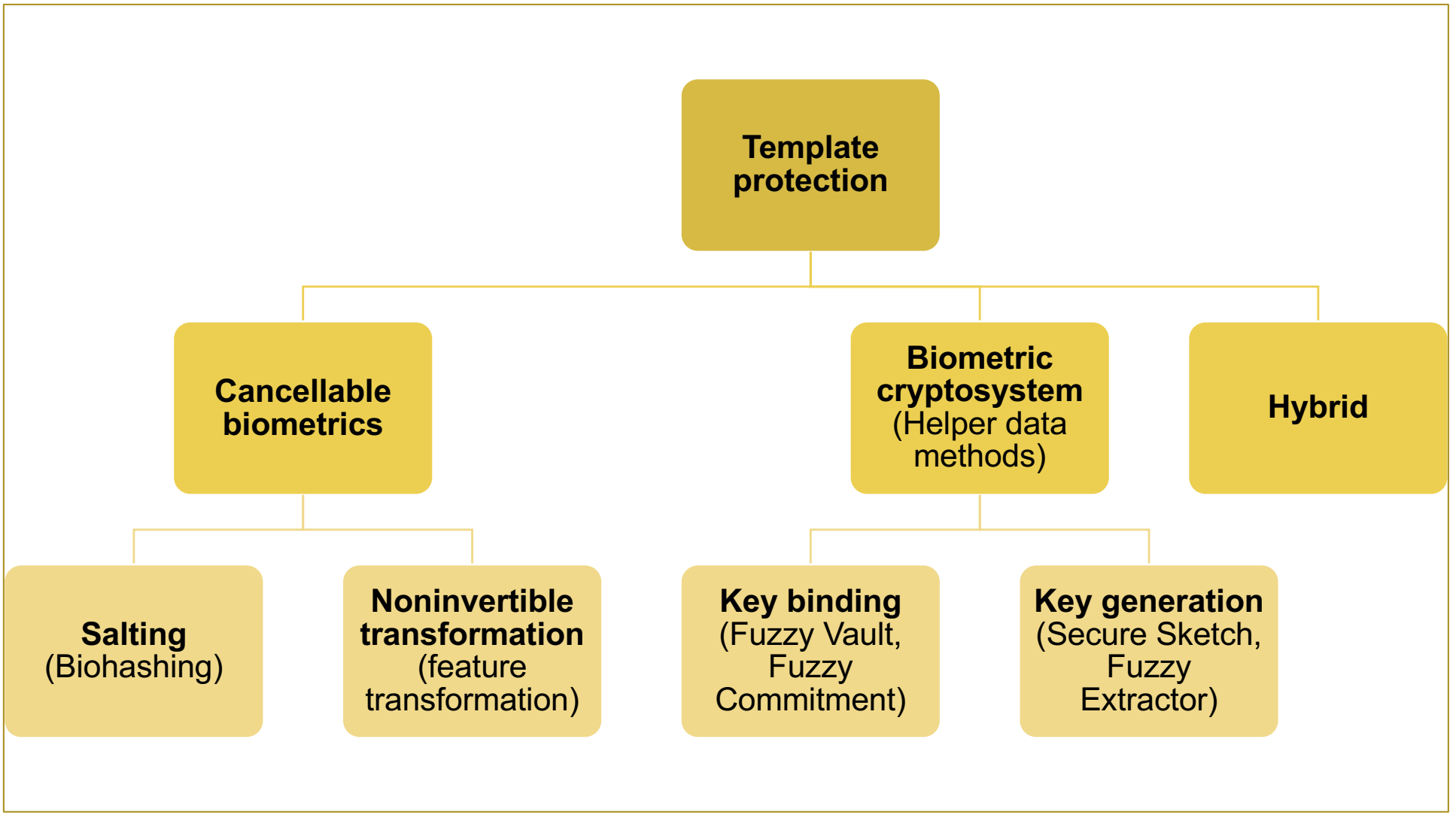
- **Attacks on the software modules:**
  - The executable program at a module can be modified such that it always outputs the values desired by the adversary
  - Countermeasure: Secure code execution practices or specialized hardware which can enforce secure execution of software should be used

Countering adversary attacks

- **Attacks on the template database:**
  - The most potentially damaging attack on a biometric system
  - A template can be replaced by an impostor's template to gain unauthorized access
  - A physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait)
  - The stolen template can be replayed to the matcher to gain unauthorized access

For the remaining parts, we particularly focus on template protection approaches

Template protection




Thank you!