CERIAS

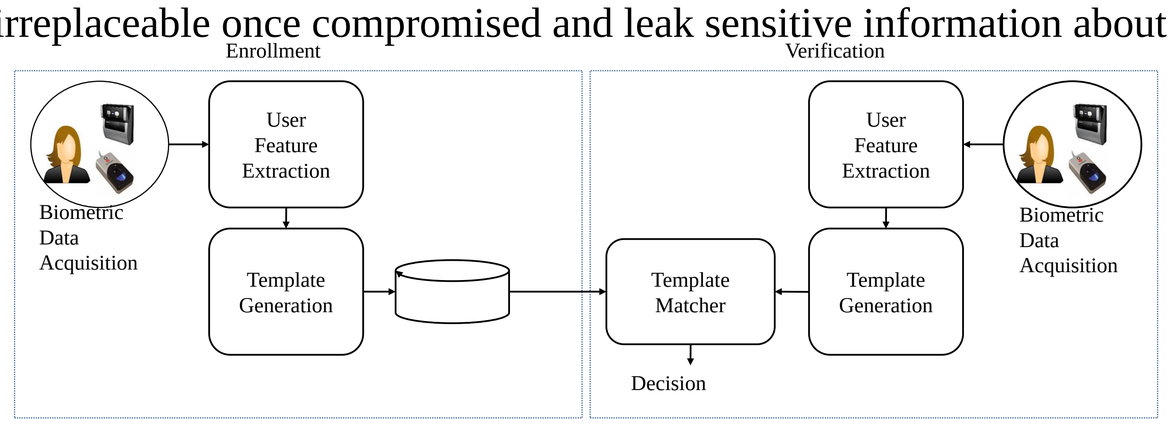
The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Resilient and active authentication and user-centric identity ecosystems

A. Problem Statement

Existing proxy based authentication approaches have problems (e.g., non-binding, susceptible to theft and dictionary attack, burden on end-users, re-use risk). Biometrics, which authenticates users by intrinsic biological traits, arises to address the drawbacks. However, the biometrics is irreplaceable once compromised and leak sensitive information about the human user behind it.

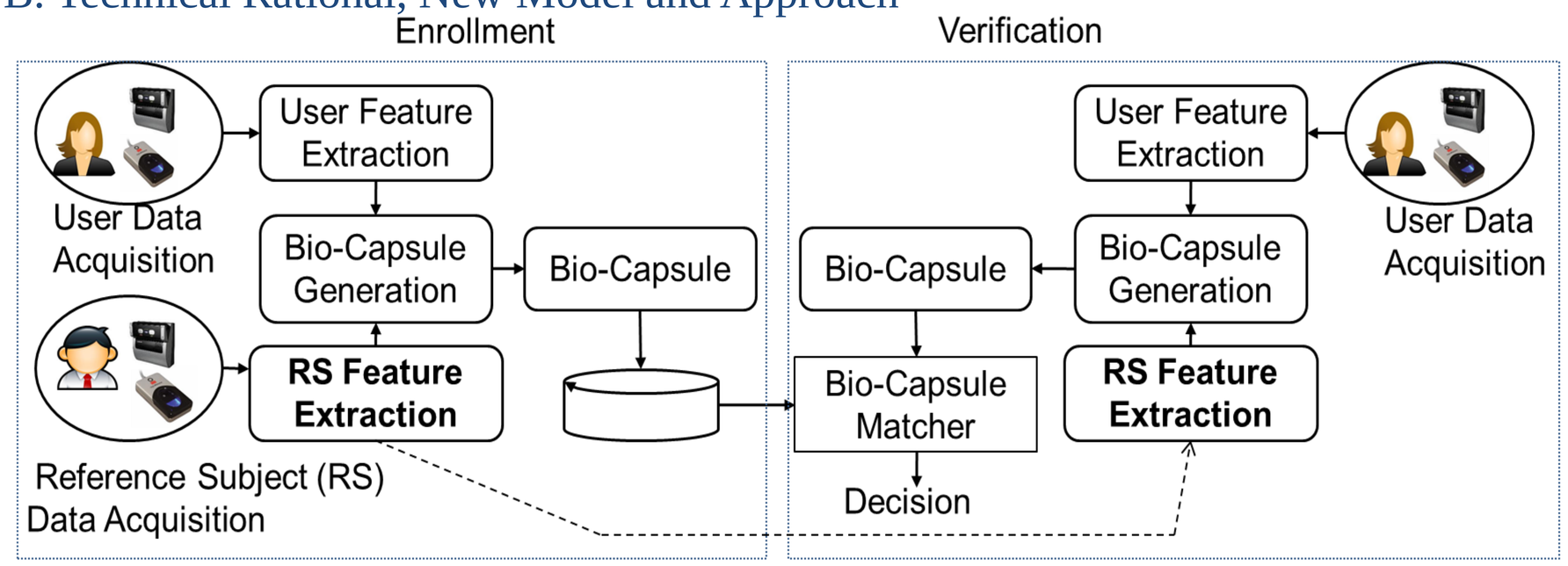


Conventional authentication system

New requirements for Biometrics:

- Diversity: do not allow cross matching across databases.
- Revocability (Cancelability): compromised template is revocable.
- Security: hard to obtain the original biometrics from secured template.
- Performance: not be degraded compared to conventional system.

B. Technical Rational, New Model and Approach

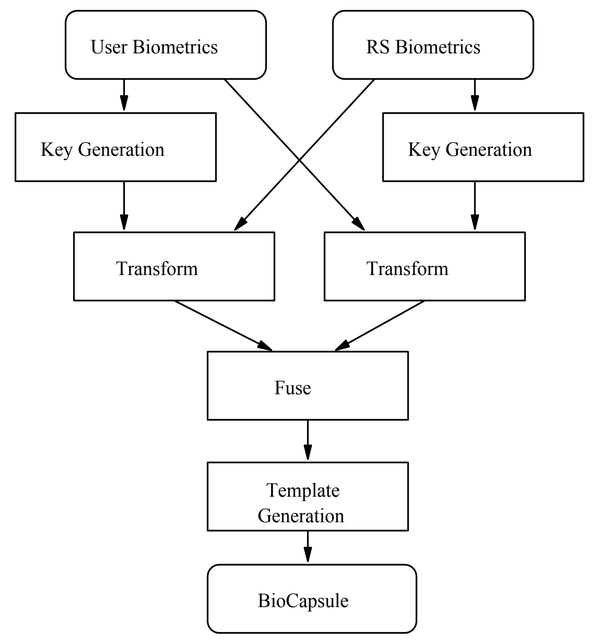


New system model

No additional user requirements for using BC (as some existing approaches does): training, additional PINs

No need for error-correct code, helper data, and no key length limitation

We propose a simple yet effective mechanism "Biometric Capsule". The proposed mechanism fuses biometrics of a user and a (physical) Reference Subject and extracts BC for authentication.



BC generation

Preliminary Result and comparisons:

DATABASE	Approach	EER	FRR(FAR = 10^{-4})
ICE (whole set)	Log Gabor	0.0108	0.0365
	Log Gabor + BC	0.0108	0.0374
ICE (quality set)	Log Gabor	0.0028	0.0063
	Log Gabor + BC	0.0030	0.0064
ICE (whole set)	2D Gabor	0.0090	0.0264
	2D Gabor + BC	0.0097	0.0291
ICE (quality set)	2D Gabor	0.0028	0.0051
	2D Gabor + BC	0.0029	0.0059

Approach	Fuzzy Commitment	Fuzzy Vault	Non-invertible Transform	Biometric Salting	Ours
Brute Force	SP	SP	NK	NK	RP
Cross Matching	SP	SP	NK	NK	RP
Collusion attack	SP	SP	SP	NK	RP
Lost Token	SP	SP	S	NK	RP

SP: Suffer Possible; NK: Not Known; RP: Resistant Proved; S: Suffer

The primary approach is to extract keys from both the user data and the RS data and properly bind the keys with the user's and RS data to perform fusion so that the fused result will not bear any hints of the user biometric information.

C. Features and Potential Applications

(a) Provably secure (b) Usable and identity-bearing: a biometric-binding identity, plus non-intrusive continuous authentication, provides traceability and mitigate liability. (c) Privacy preserving (d) Biometric cancelable (e) General applicable: working with existing biometric modules. (f) Interoperable: supports "one-click sign on" across multiple systems by using a distinct RS on each system. (g) Cost-effective and easy to use: transparent to end-users, no user training.

User-centric identity ecosystem: the new BC based model is promising in developing a highly resilient, privacy-preserving, revocable, interoperable, and efficient user-centric identity verification and protection ecosystem.

Active authentication system: the new BC based approach is encouraging in developing a provably secure, privacy-preserving, biometric active authentication system to support continuous and non-intrusive authentication.

Student: Yan Sui (ysui@iupui.edu) Major Professor: Dr. Xukai Zou (xkzou@cs.iupui.edu)

CERIAS

Discovery Park e-Enterprise Center