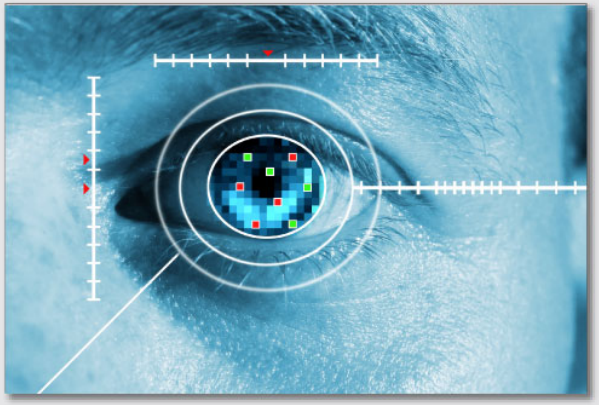
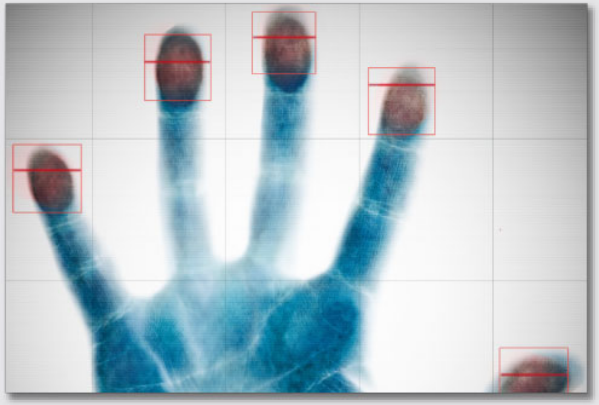
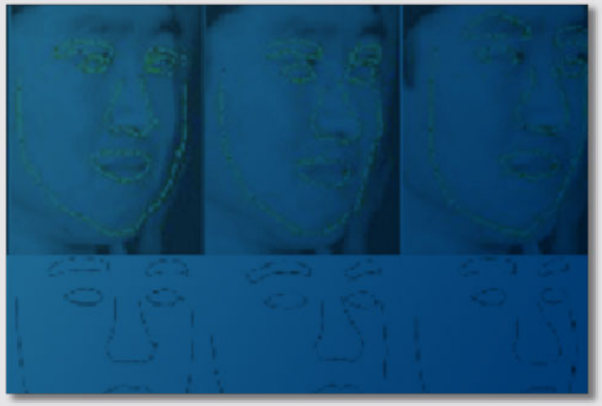
CITeR
CENTER FOR IDENTIFICATION TECHNOLOGY RESEARCH

A National Science Foundation Industry/University Cooperative Research Center

Mobile Biometrics in the Cloud

Matthew Valenti, Ph.D., P.E.
West Virginia University

Oct. 30, 2014

Outline

1. Introduction: Biometrics and the cloud
2. Walkthrough of a cloud-based identification application
3. Mobile interfaces
4. A marketplace for algorithms
5. Conclusion

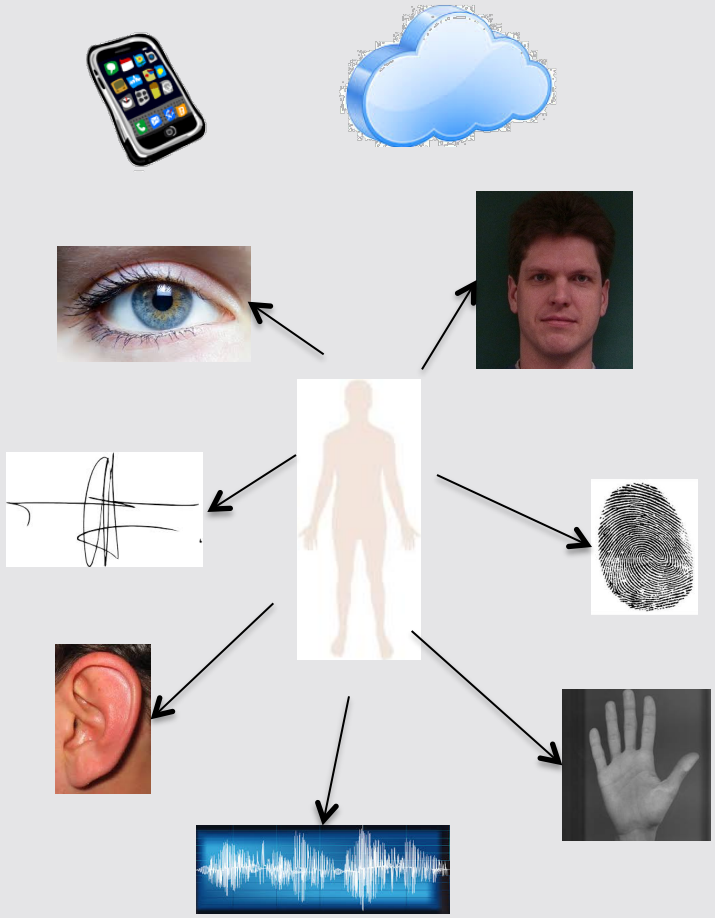
Outline

1. **Introduction: Biometrics and the cloud**
2. Walkthrough of a cloud-based identification application
3. Mobile interfaces
4. A marketplace for algorithms
5. Conclusion

Motivation

The Synergies Between Biometrics, Cloud, and Mobile

- The cloud provides unbounded, cost-effective, and elastic computing resources.
- Biometrics can leverage the efficiency of the cloud.
- The cloud provides an opportunity to offload compute-intensive operations from the mobile device.
- Conversely, biometrics can help to make the cloud more secure.



Challenges and Opportunities

- Challenges
  - How to adapt biometric algorithms to the cloud?
  - How to preserve the privacy of individual's biometric data?
  - How to provide useful interfaces and mobile applications?
- Opportunities
  - Cloud computing reduces the need for a biometric service provider to maintain their own infrastructure.
  - Emergence of a new business models:
    Biometric Authentication as a Service (**BioAaaS**)
    Biometric Enabled Mobile Applications
    Algorithm Marketplace

Biometrics Leveraging the Cloud

- Using the cloud to perform biometric matching & computation
  - Rapid analytics: e.g., identification through parallelization.
  - "Big data" biometrics using Hadoop, ZooKeeper, and Accumulo.
- Using the cloud to store biometric data.
  - The cloud is a cost effective and elastic way to store and share data.
  - Need to preserve privacy of biometric data while in the cloud, and during transfer to/ from the cloud.
  - Potential to support access from different entities under different policies.
  - Laws may dictate where the data is stored.
  - Potential to share biometric data among research organizations.
- Biometrics as a service
  - Allow access to different algorithms provided by different service providers and/or developers.
  - Upload the algorithm, not the biometric.

The Cloud Leveraging Biometrics

- Biometrics can be used by cloud service providers to provide new security features.
- Use cases:
  - Biometric authentication for cloud clients.
    - e.g., Cloud Iris Verification System (CIVS), Kesava, 2010, Correlation keystroke verification, Xi et al., 2011.
  - Securing cloud data storage with biometrics.
    - Biocryptographic systems
    - Using biometrics for key generation: Fuzzy extractor.
    - Using biometrics for key binding: Fuzzy vault, Fuzzy commitment, Bipartite token.
  - Authentication as a service (AaaS)
    - Outsource system authentication to the cloud.
    - Confederates access to a single sign-on.

Security Threats

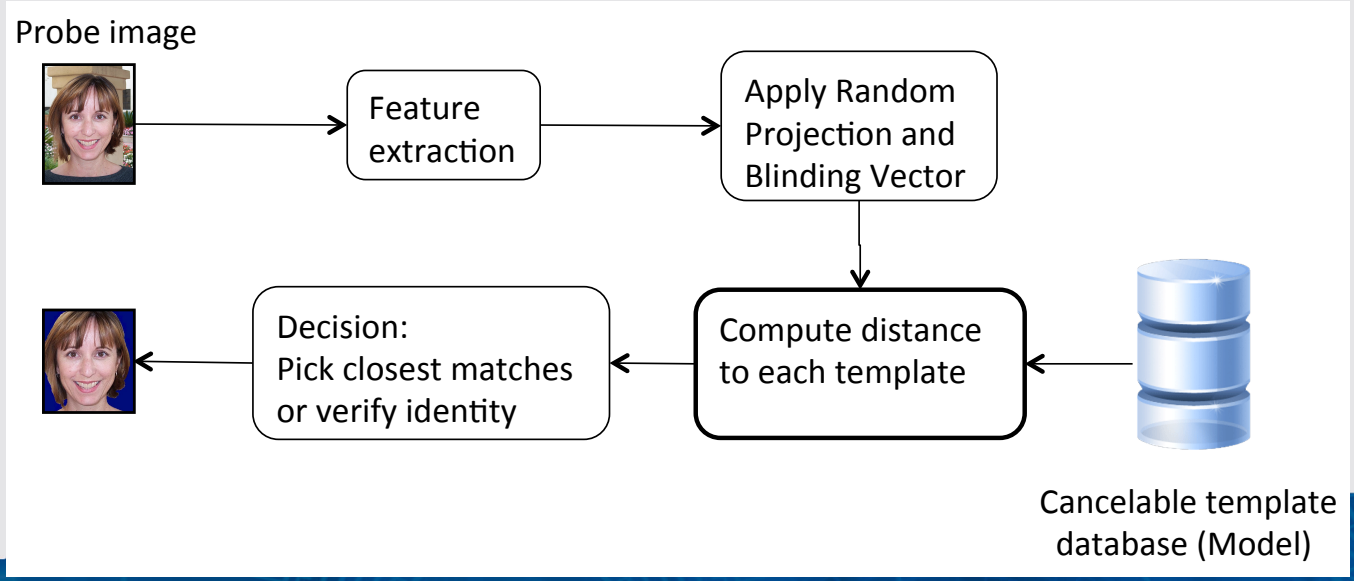
- Biometric dilemma threat
  - Attacker compromises a less secure system to obtain biometric data.
  - Then uses the biometric data to gain access to a secure, high-value system.
- Doppleganger threat
  - Attacker presents a large amount of biometric data, in the hopes of achieving a match.
  - Exploits non-zero False Accept Rates (FAR)
  - Analogous to a dictionary attack.
- Trust Issues
  - Who is allowed to enroll the users?

Outline

1. Introduction: Biometrics and the cloud
2. **Walkthrough of a cloud-based identification application**
3. Mobile interfaces
4. A Marketplace for Algorithms
5. Conclusion

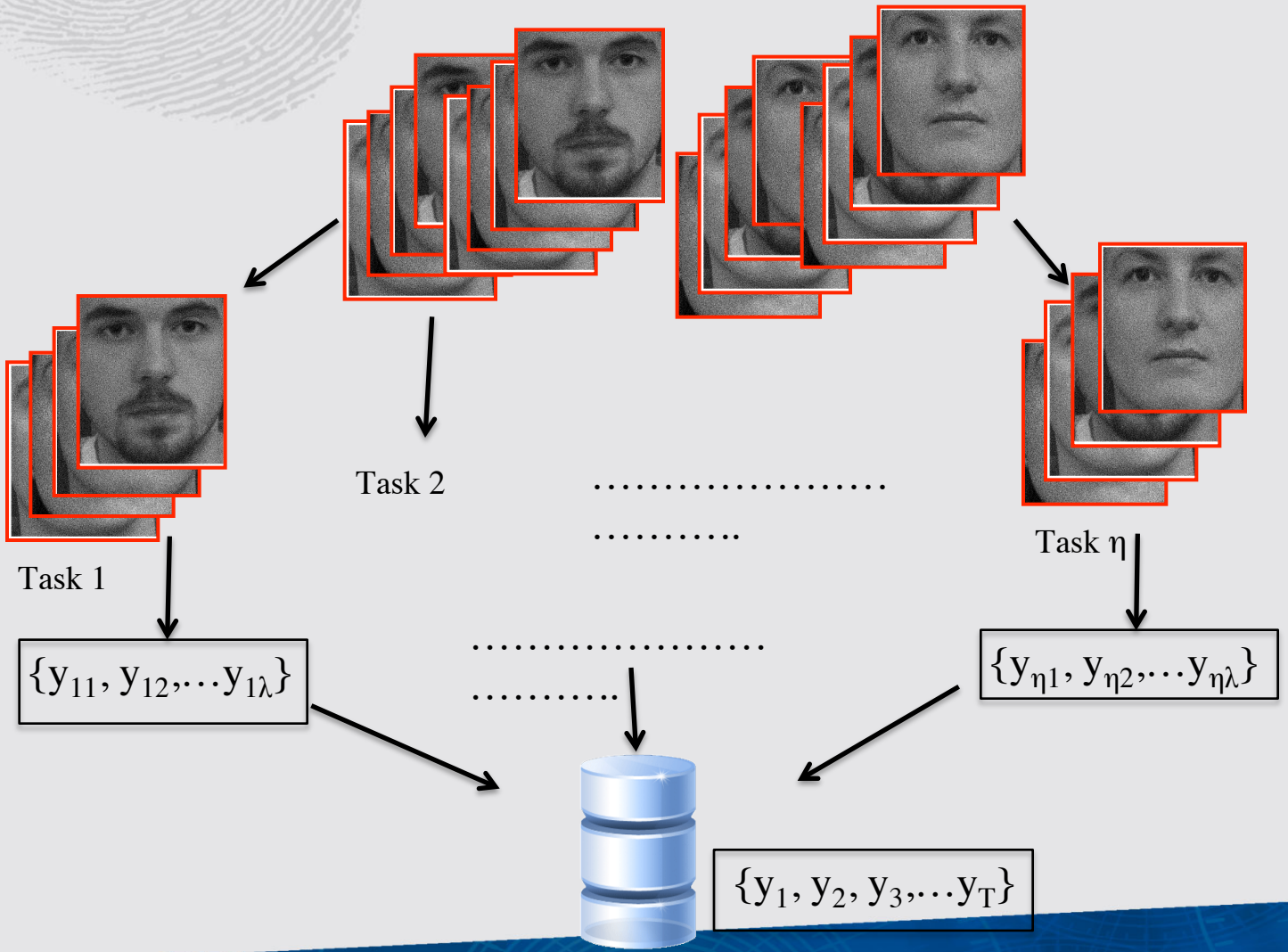
A Proof-of-Concept Demo

- To demonstrate the concept of cloud biometrics a mobile app was developed, featuring:
  - Facial recognition based on the LBP algorithm.
  - Parallel enrolment and matching on a virtual private cloud.
  - Cancelable biometric database for privacy preservation.
  - Smartphone app implemented as a mobile-friendly web application.



Parallel System Implementation

Biometric Template Generation



Face images database

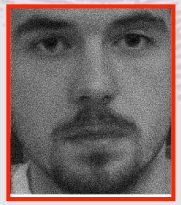
Task division

Generate cancelable templates

Cancelable template data model

Parallel System Implementation

Parallel Distance Matching



Probe image

Cancelable template, z

Model

Preprocessing

$(z, \{y_1, y_2, y_3, \ldots y_T\})$

Task division

$(z, \{y_{11}, y_{12}, \ldots y_{1\lambda}\})$

Task 1

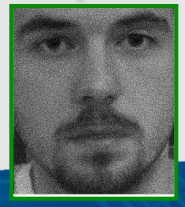
$(z, \{y_{\eta 1}, y_{\eta 2}, \ldots y_{\eta\lambda}\})$

Task η

$\{d_{11}, d_{12}, \ldots d_{1\lambda}\})$

$\{d_{\eta 1}, d_{\eta 2}, \ldots d_{\eta\lambda}\}$

Calculate distance



Establish identity

Outline

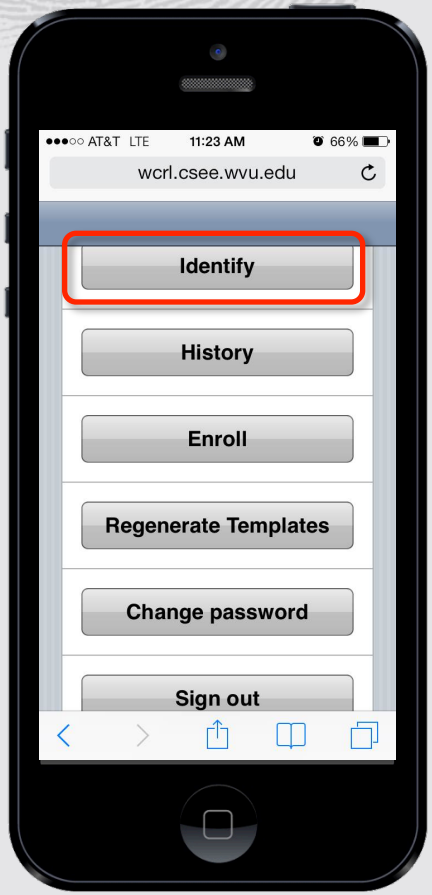
1. Introduction: Biometrics and the cloud
2. Walkthrough of a cloud-based identification application
3. **Mobile interfaces**
4. A Marketplace for Algorithms
5. Conclusion

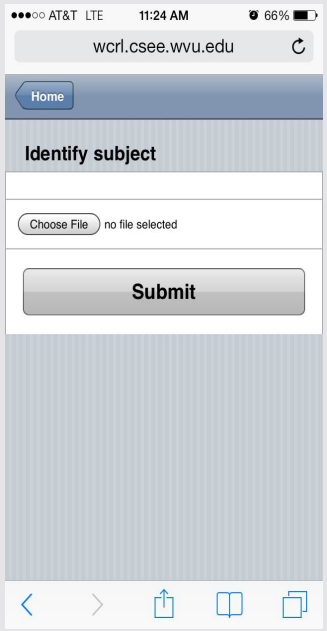
A Typical Smart-Phone Interface

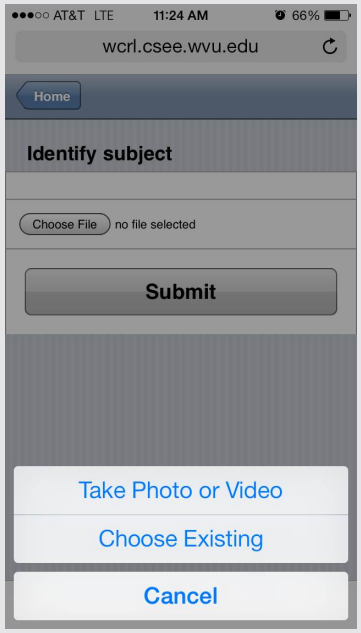
Mobile application --- Login screen

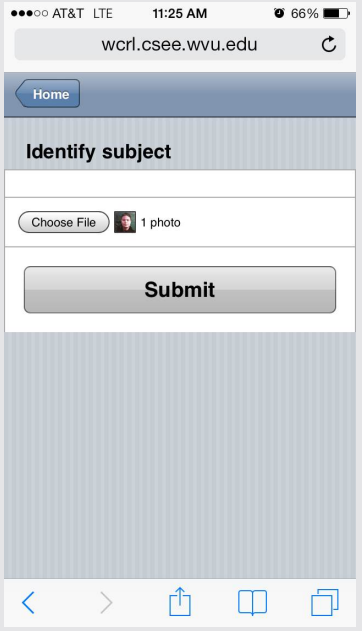
A Typical Smart-Phone Interface

Mobile application --- Identification



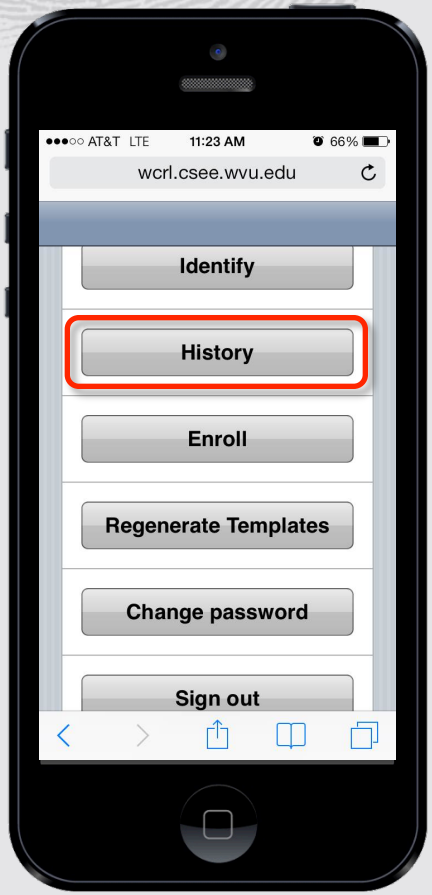






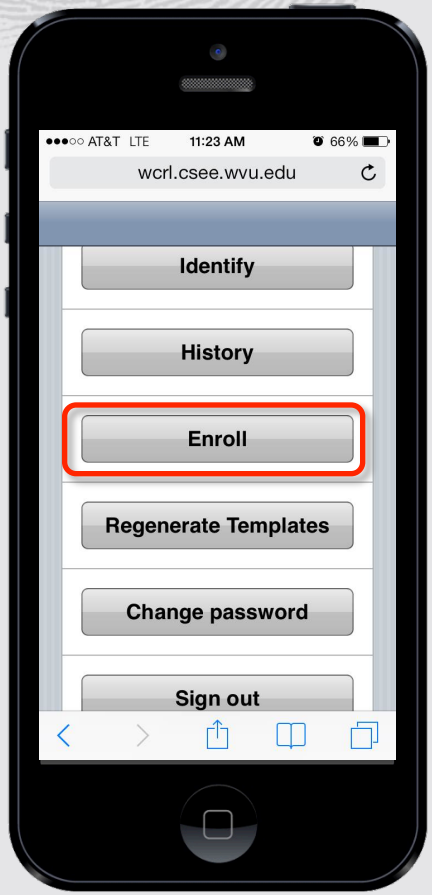
A Typical Smart-Phone Interface

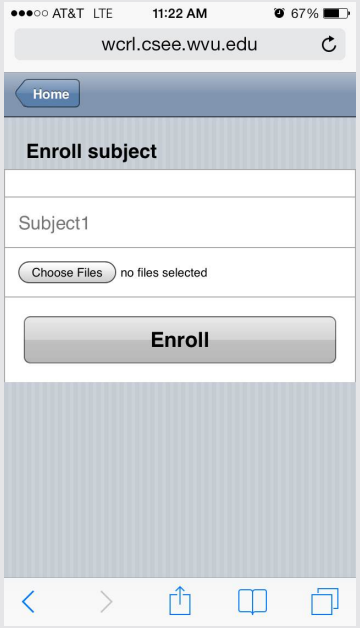
Mobile application --- Job History

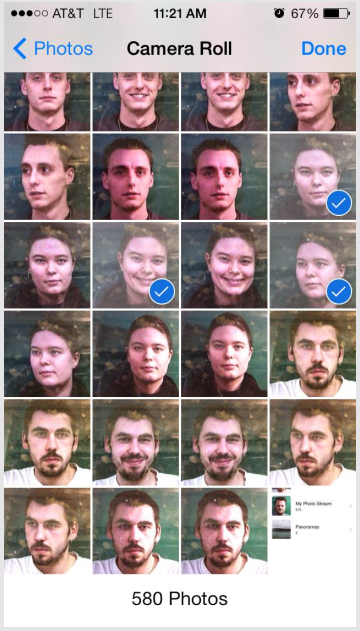


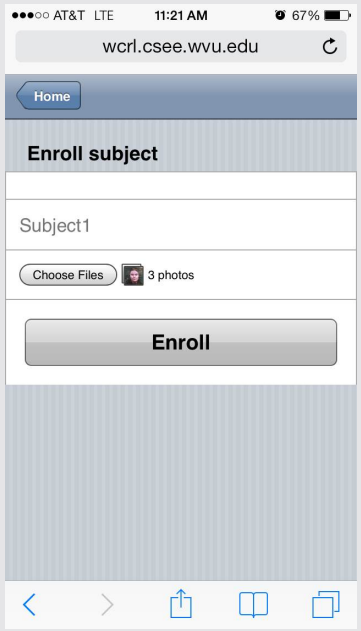
A Typical Smart-Phone Interface

Mobile application --- Enroll a Subject



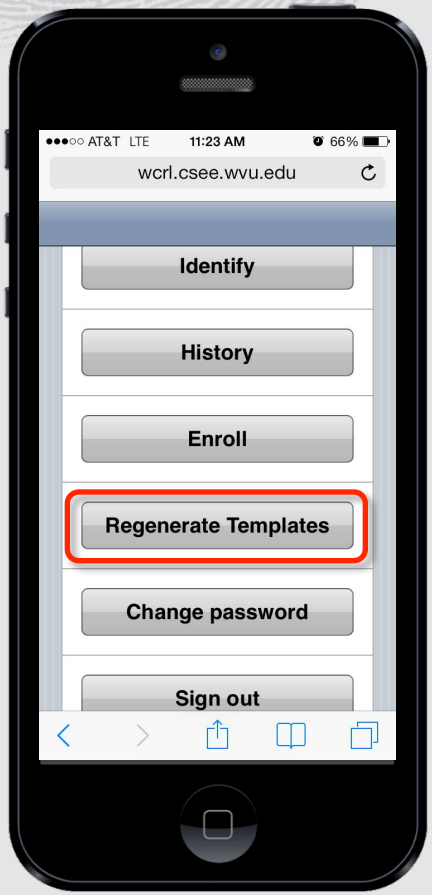


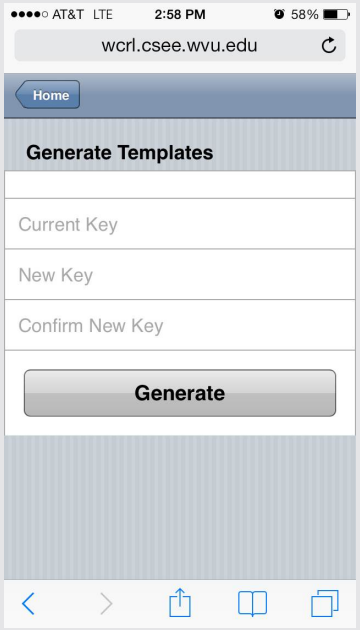




A Typical Smart-Phone Interface

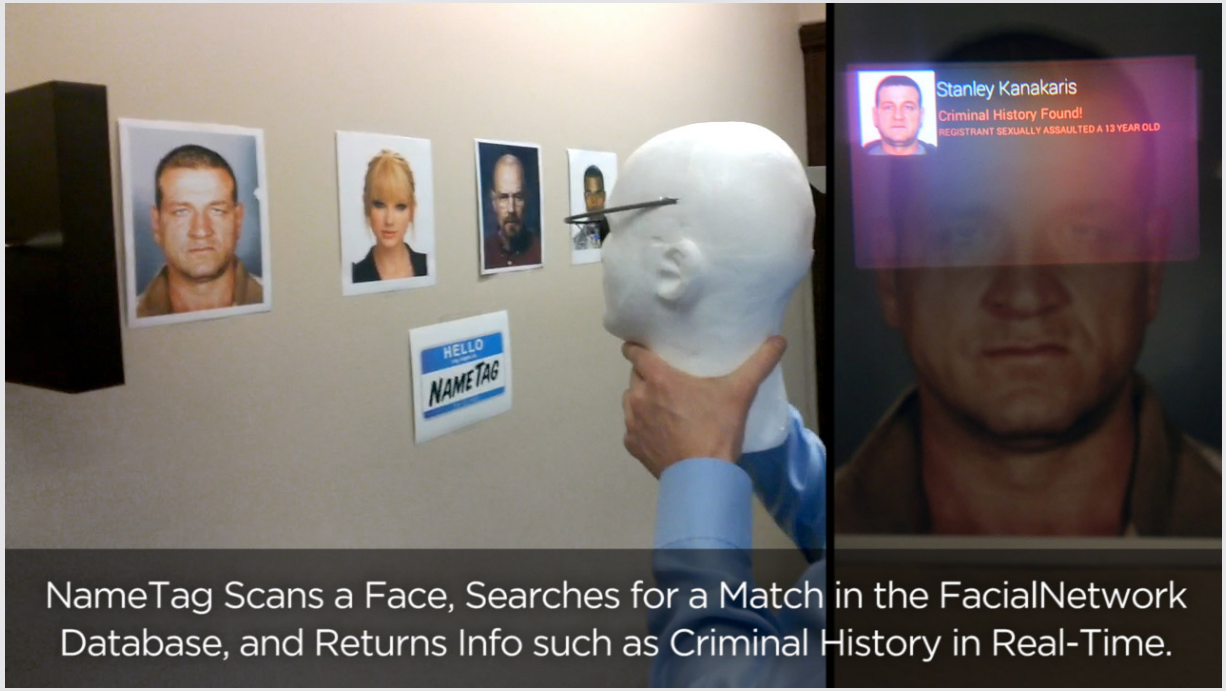
Mobile application --- Regenerate Template





Other Interfaces

- Google glass is a good platform for recognition applications.



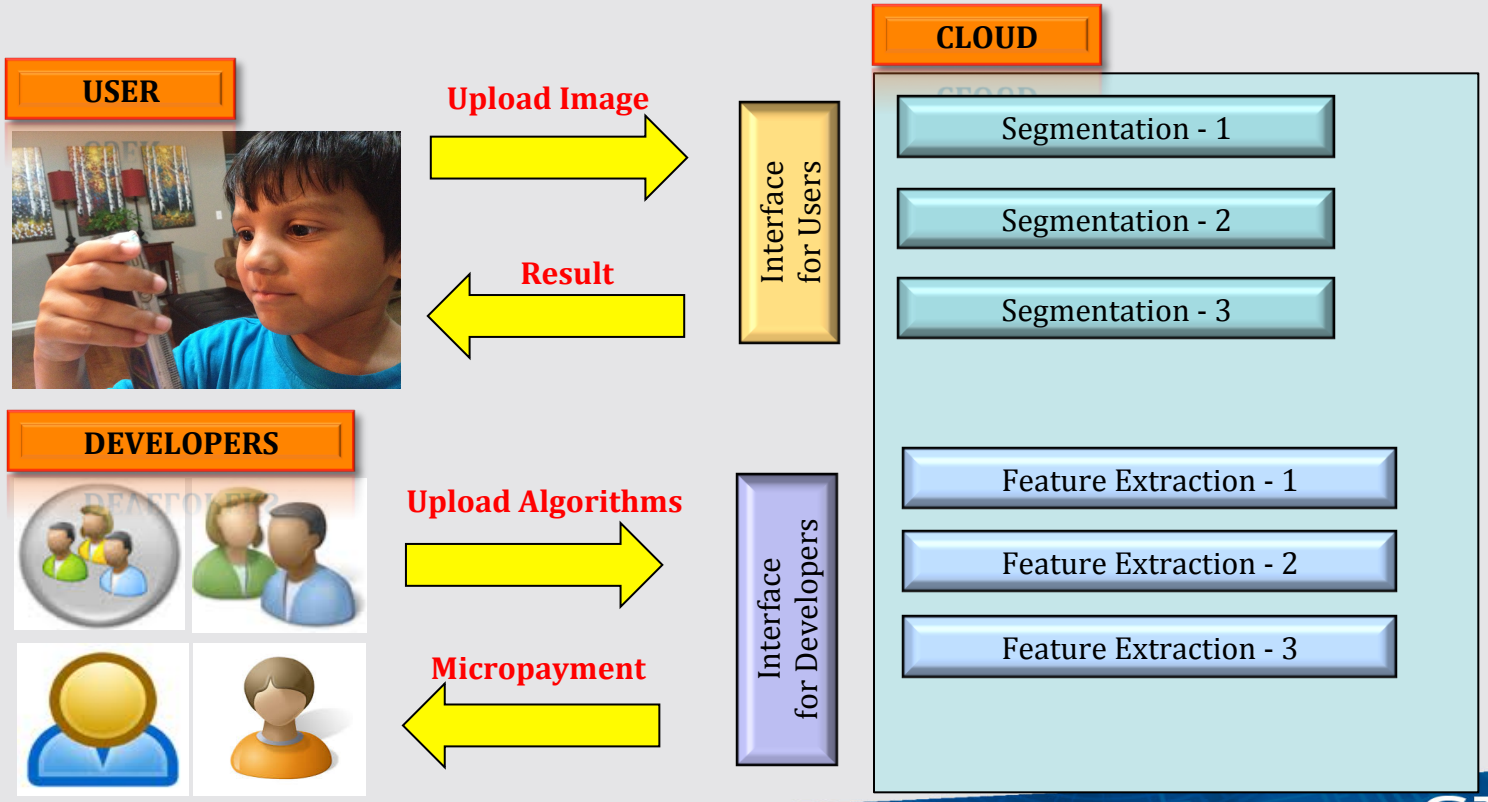
Outline

1. Introduction: Biometrics and the cloud
2. Walkthrough of a cloud-based identification application
3. Mobile interfaces
4. **A marketplace for algorithms**
5. Conclusion

The Developer's Perspective

An Algorithm Marketplace

- Developers should be provided interfaces to upload their algorithms to the cloud.
- This results in new business models, where individual algorithm developers are provided with an opportunity to receive financial incentive



Outline

1. Introduction: Biometrics and the cloud
2. Parallel identification in the cloud
3. Mobile interfaces
4. A marketplace for algorithms
5. **Conclusion**

Conclusions

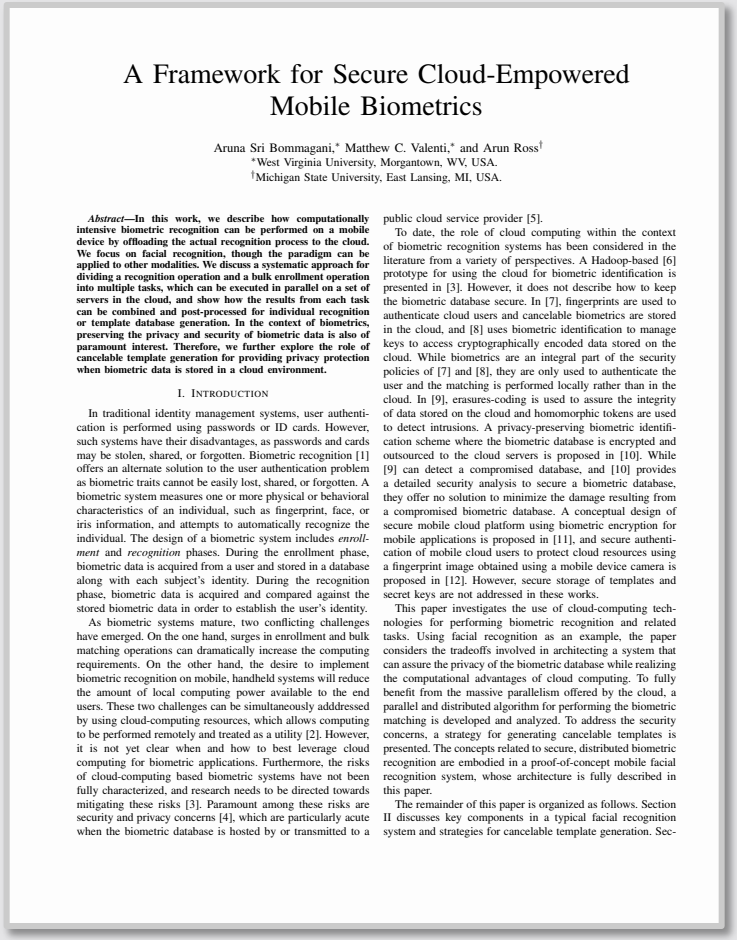
- The limitless computational resources of the cloud can be used to empower mobile biometric applications.
- Care should be taken to protect identity when biometrics are stored in the cloud.
- New applications and business models will follow.

For More Information

A.S. Bommagani, M.C. Valenti, and A. Ross, "A framework for secure cloud-empowered mobile biometrics," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, (Baltimore, MD), Oct. 2014.

Available online at:

http://www.csee.wvu.edu/~mvalenti



A Framework for Secure Cloud-Empowered Mobile Biometrics

Aruna Sri Bommagani,* Matthew C. Valenti,* and Arun Ross†
*West Virginia University, Morgantown, WV, USA.
†Michigan State University, East Lansing, MI, USA.

***Abstract*—In this work, we describe how computationally intensive biometric recognition can be performed on a mobile device by offloading the actual recognition process to the cloud. We focus on facial recognition, though the paradigm can be applied to other modalities. We discuss a systematic approach for dividing a recognition operation and a bulk enrollment operation into multiple tasks, which can be executed in parallel on a set of servers in the cloud, and show how the results from each task can be combined and post-processed for individual recognition or template database generation. In the context of biometrics, preserving the privacy and security of biometric data is also of paramount interest. Therefore, we further explore the role of cancelable template generation for providing privacy protection when biometric data is stored in a cloud environment.**

I. Introduction

In traditional identity management systems, user authentication is performed using passwords or ID cards. However, such systems have their disadvantages, as passwords and cards may be stolen, shared, or forgotten. Biometric recognition [1] offers an alternate solution to the user authentication problem as biometric traits cannot be easily lost, shared, or forgotten. A biometric system measures one or more physical or behavioral characteristics of an individual, such as fingerprint, face, or iris information, and attempts to automatically recognize the individual. The design of a biometric system includes *enrollment* and *recognition* phases. During the enrollment phase, biometric data is acquired from a user and stored in a database along with each subject's identity. During the recognition phase, biometric data is acquired and compared against the stored biometric data in order to establish the user's identity.

As biometric systems mature, two conflicting challenges have emerged. On the one hand, surges in enrollment and bulk matching operations can dramatically increase the computing requirements. On the other hand, the desire to implement biometric recognition on mobile, handheld systems will reduce the amount of local computing power available to the end users. These two challenges can be simultaneously adddressed by using cloud-computing resources, which allows computing to be performed remotely and treated as a utility [2]. However, it is not yet clear when and how to best leverage cloud computing for biometric applications. Furthermore, the risks of cloud-computing based biometric systems have not been fully characterized, and research needs to be directed towards mitigating these risks [3]. Paramount among these risks are security and privacy concerns [4], which are particularly acute when the biometric database is hosted by or transmitted to a public cloud service provider [5].

To date, the role of cloud computing within the context of biometric recognition systems has been considered in the literature from a variety of perspectives. A Hadoop-based [6] prototype for using the cloud for biometric identification is presented in [3]. However, it does not describe how to keep the biometric database secure. In [7], fingerprints are used to authenticate cloud users and cancelable biometrics are stored in the cloud, and [8] uses biometric identification to manage keys to access cryptographically encoded data stored on the cloud. While biometrics are an integral part of the security policies of [7] and [8], they are only used to authenticate the user and the matching is performed locally rather than in the cloud. In [9], erasures-coding is used to assure the integrity of data stored on the cloud and homomorphic tokens are used to detect intrusions. A privacy-preserving biometric identification scheme where the biometric database is encrypted and outsourced to the cloud servers is proposed in [10]. While [9] can detect a compromised database, and [10] provides a detailed security analysis to secure a biometric database, they offer no solution to minimize the damage resulting from a compromised biometric database. A conceptual design of secure mobile cloud platform using biometric encryption for mobile applications is proposed in [11], and secure authentication of mobile cloud users to protect cloud resources using a fingerprint image obtained using a mobile device camera is proposed in [12]. However, secure storage of templates and secret keys are not addressed in these works.

This paper investigates the use of cloud-computing technologies for performing biometric recognition and related tasks. Using facial recognition as an example, the paper considers the tradeoffs involved in architecting a system that can assure the privacy of the biometric database while realizing the computational advantages of cloud computing. To fully benefit from the massive parallelism offered by the cloud, a parallel and distributed algorithm for performing the biometric matching is developed and analyzed. To address the security concerns, a strategy for generating cancelable templates is presented. The concepts related to secure, distributed biometric recognition are embodied in a proof-of-concept mobile facial recognition system, whose architecture is fully described in this paper.

The remainder of this paper is organized as follows. Section II discusses key components in a typical facial recognition system and strategies for cancelable template generation. Sec-