A Framework for Secure Cloud-Empowered Mobile Biometrics

A. Bommagani[1], M. C. Valenti[1], and A. Ross[2]
[1]West Virginia University, Morgantown, WV, USA
[2]Michigan State University, East Lansing, MI, USA

This research was funded by the Center for Identification Technology Research (CITeR), a National Science Foundation (NSF) Industry/University Cooperative Research Center (I/UCRC).

Oct. 7th, 2014

Outline

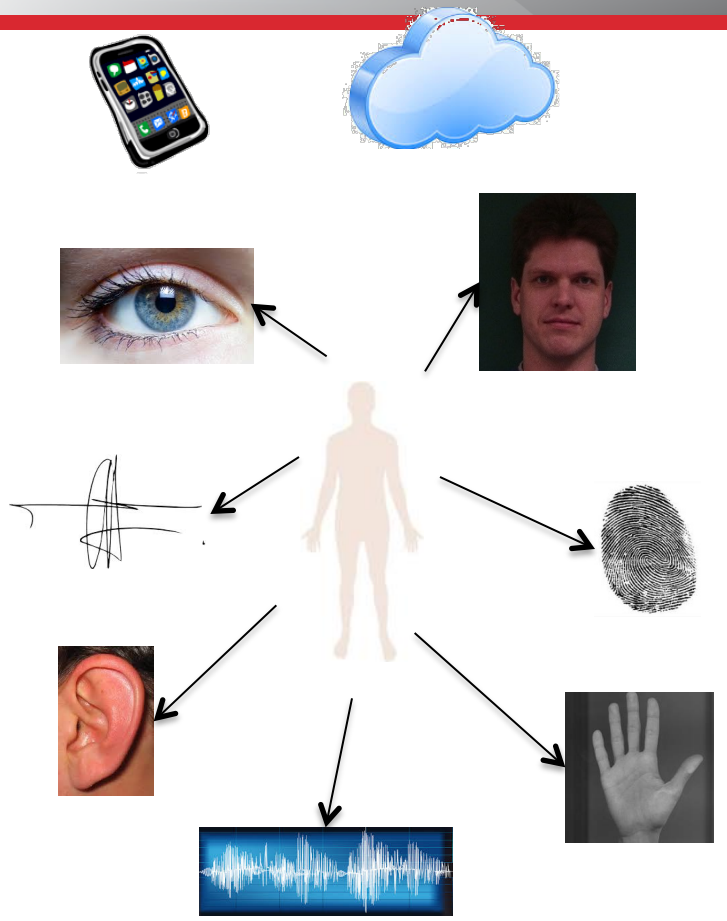
1. Introduction
2. Homomorphic LBP-based face recognition
3. A framework for secure cloud biometrics
4. System analysis
5. Conclusion

Outline

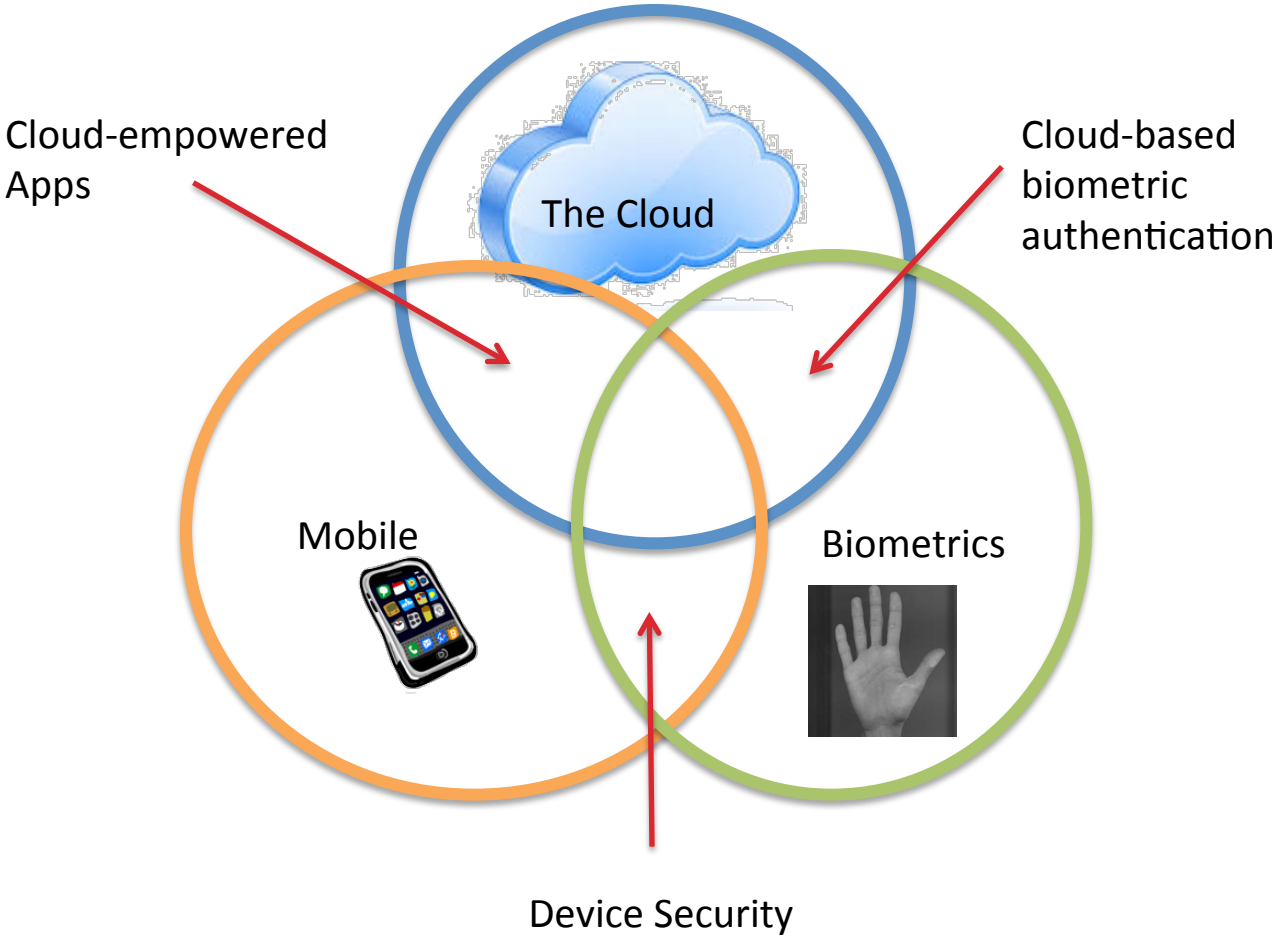
1. **Introduction**
2. Homomorphic LBP-based face recognition
3. A framework for secure cloud biometrics
4. System analysis
5. Conclusion

Introduction

- 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.



Mobile + Cloud + Biometrics



The Cloud leveraging Biometrics

- 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?

Biometrics leveraging the Cloud

- 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.
- Using the cloud to perform biometric computations
  - Rapid analytics: e.g., identification through parallelization.
  - "Big data" biometrics using Hadoop, ZooKeeper, and Accumulo.
- Biometrics as a service
  - Allow access to different algorithms provided by different service providers and/or developers.
  - Upload the algorithm, not the biometric.

Literature review

- A Hadoop-based prototype for using the cloud for biometric identification is proposed in [3], but it does not describe biometric database security.
- Fingerprint authentication and storage of cancelable biometrics in the cloud is proposed in [7]. However, in this work matching is performed locally.
- A privacy-preserving biometric identification scheme is proposed in [10]. However, it does not offer a solution to minimize the damage resulting from a compromised biometric database.
- Secure authentication of mobile cloud users using a fingerprint image (using a mobile device camera) is proposed in [12], but data security is not addressed in this work.

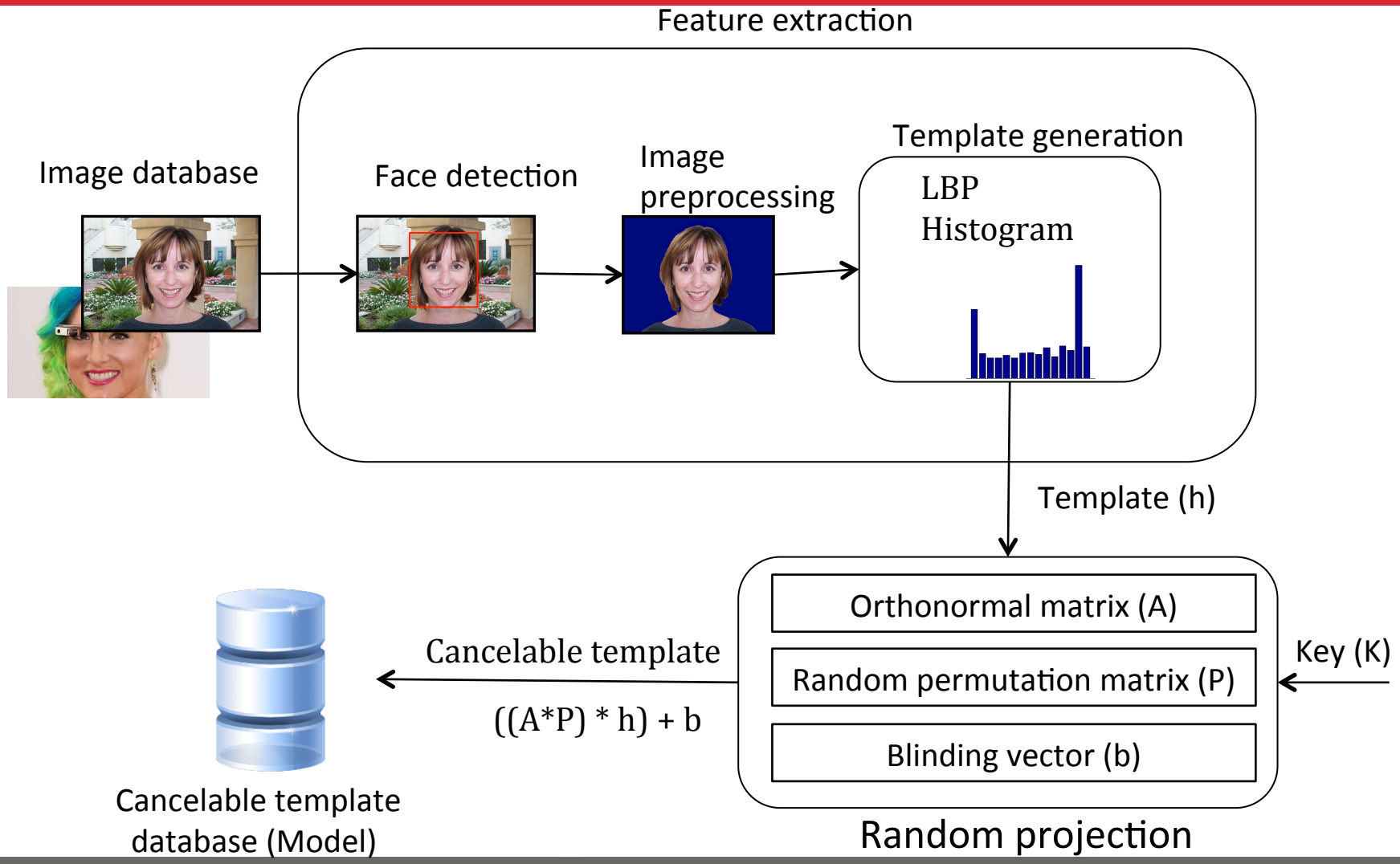
Outline

1. Introduction
2. **Homomorphic LBP-based face recognition**
3. A framework for secure cloud biometrics
4. System analysis
5. Conclusion

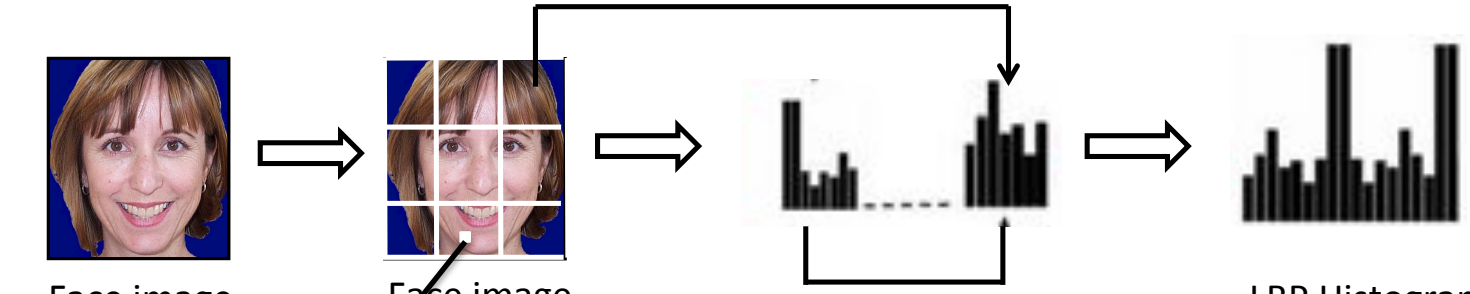
Motivation and Goals

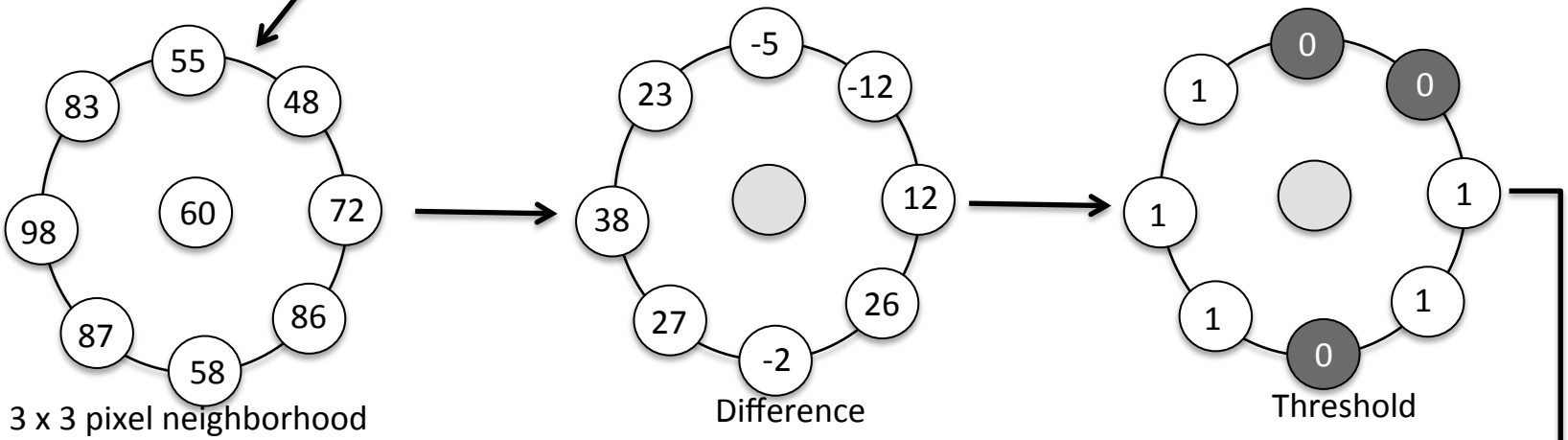
- There is a need to know when and how to best leverage cloud computing for biometric applications.
- There is also a need to characterize the risks and benefits of using cloud computing for biometric systems.
- Goal: To demonstrate the ability to leverage CC services for mobile biometrics, while still maintaining the privacy of the underlying biometric database.
- Developed a proof of concept demo featuring:
  - Facial recognition based on the LBP algorithm.
  - Homomorphic templates to protect privacy of individual's biometrics.

Enrollment – Secure model generation



Local Binary Patterns (LBP)-based template generation





$236 = (2^7*1 + 2^6*1 + 2^5*1 + 2^4*0 + 2^3*1 + 2^2*1 + 2^1*0 + 2^0*0)$ ← $(11101100)_2$

Template generation contd.,

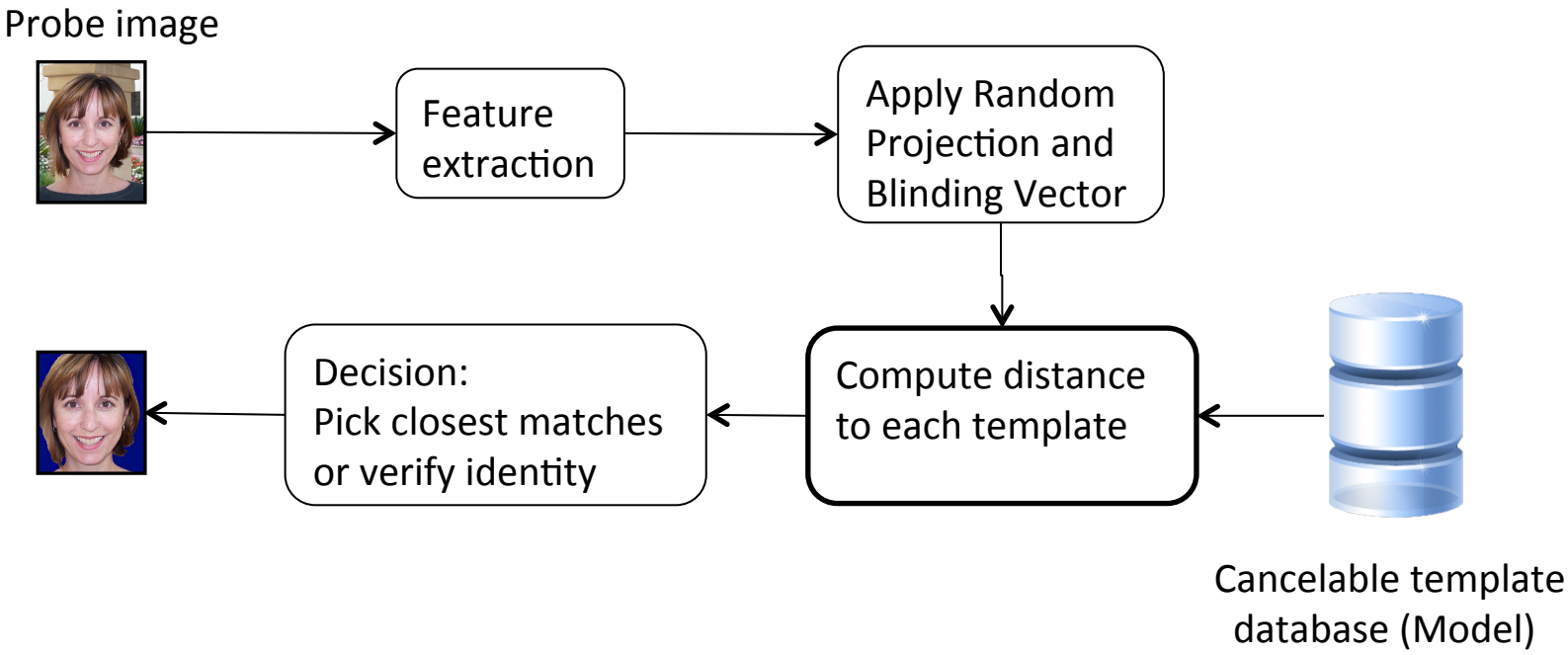
- **Uniform LBP**
  - e.g. 01110000, 11001111 ➔ at most 2 bitwise transitions
  - Each uniform pattern a separate label.
  - All non uniform patterns have a single label.
  - Total labels: P (P − 1) + 3; P = # neighbors

Template generation contd.,

- **Cancelable template generation:** cancelable template for template, h is generated using,
  - an l x l orthonormal matrix, A.
  - (for additional security, an l x l *secret permutation matrix, P* and a length l *blinding vector, b).*

$$y = \left(AP\right)h + b = Qh + b$$

Face recognition



Transformed template matching

- For a transformed probe template, z = Qx+b, and a transformed gallery template y_j, Euclidean distance is

$$d_j^2 = \left\| z - y_j \right\|$$

- Distance between templates before and after transformation is preserved because of orthogonal nature of matrix Q.
- The closest image $\hat{I}_j$

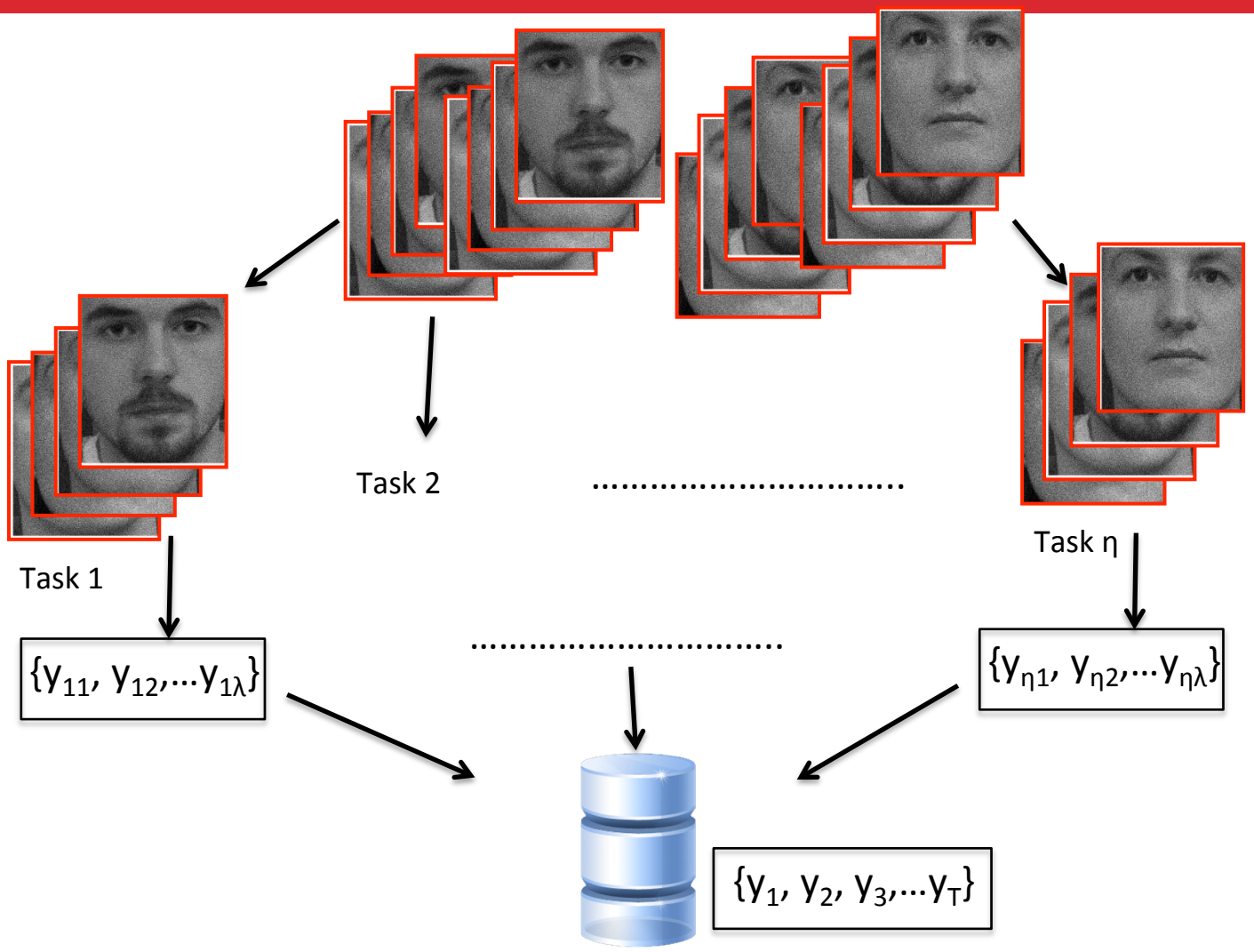
$$j = \arg\min_j \left\{ d_j \right\}$$

- Identification
  - The subject corresponding to the closest template.
  - A ranked list of matches can be provided to the user.

Outline

1. Introduction
2. Homomorphic LBP-based face recognition
3. **A framework for secure cloud biometrics**
4. System analysis
5. Conclusion

Parallel biometric template generation



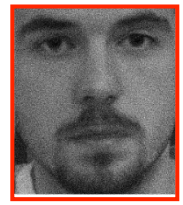
1. Face images database

2. Task division

3. Generate cancelable templates

4. Cancelable template data model

Parallel distance matching



Probe image

Cancelable template, z

Model

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

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

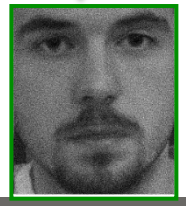
Task 1

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

Task η

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

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



1. Preprocessing

2. Task division

3. Calculate distance

4. Establish identity

System framework

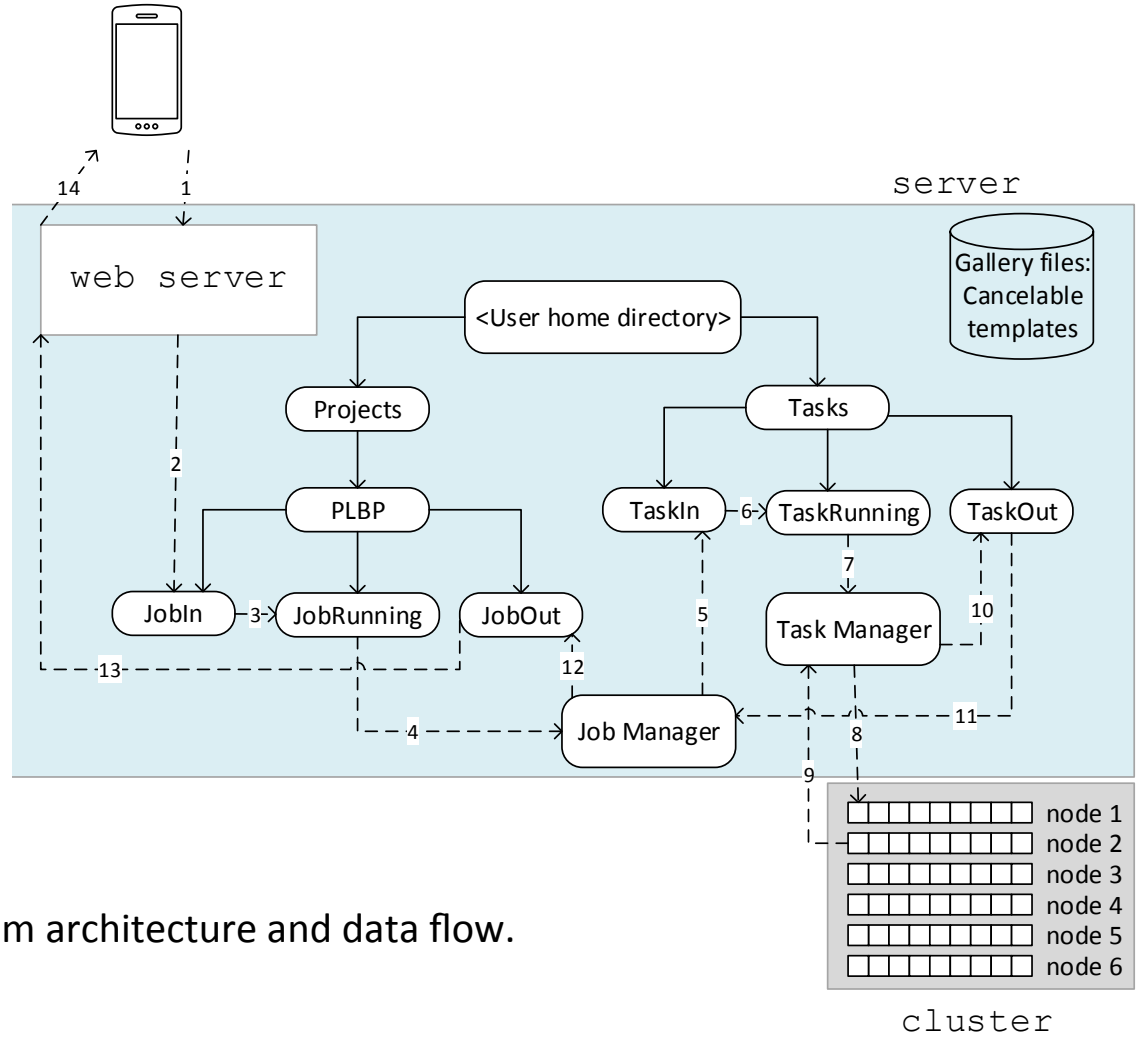
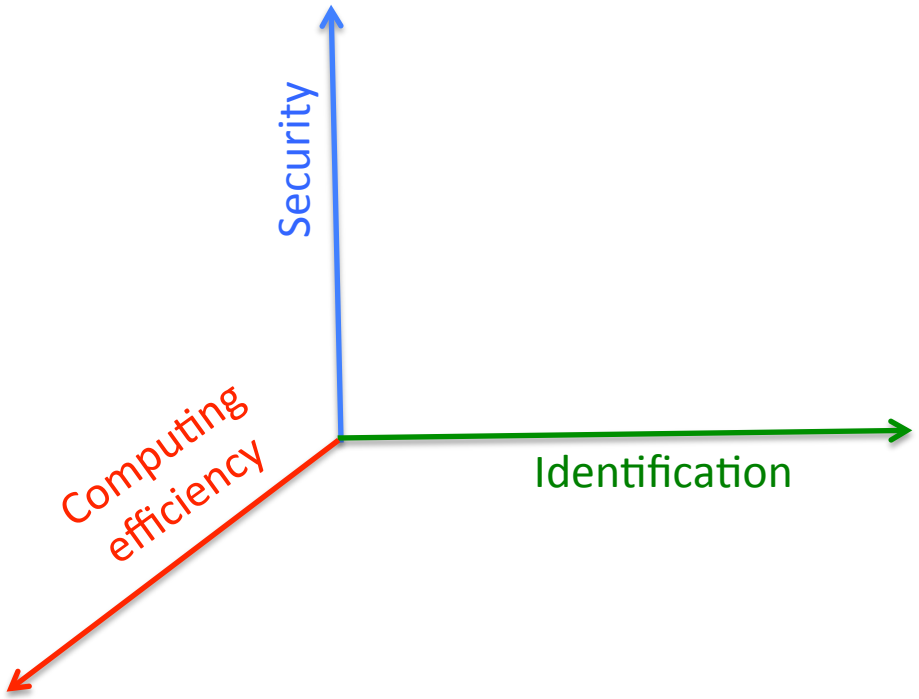


Figure: System architecture and data flow.

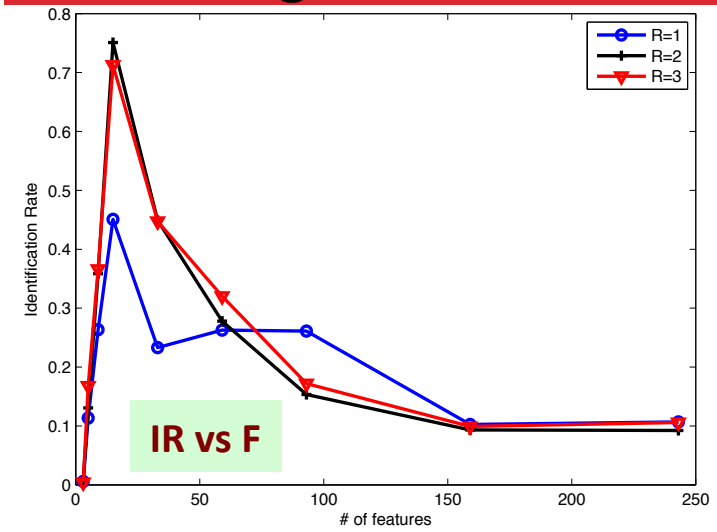
Outline

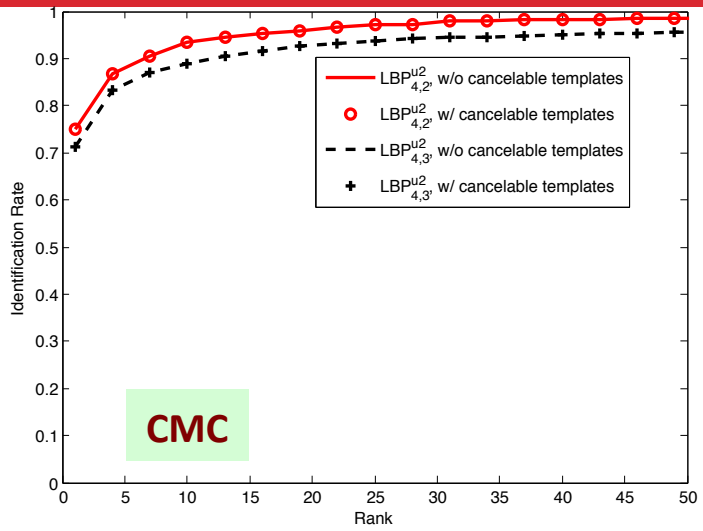
1. Introduction
2. Homomorphic LBP-based face recognition
3. A framework for secure cloud biometrics
4. **System analysis**
5. Conclusion

System analysis

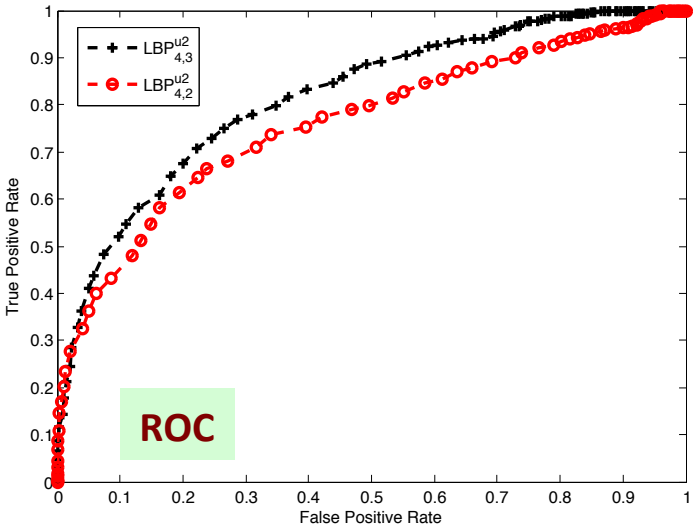


Identification system analysis -XM2VTS database and uniform LBP algorithm





Cumulative match characteristic (CMC)

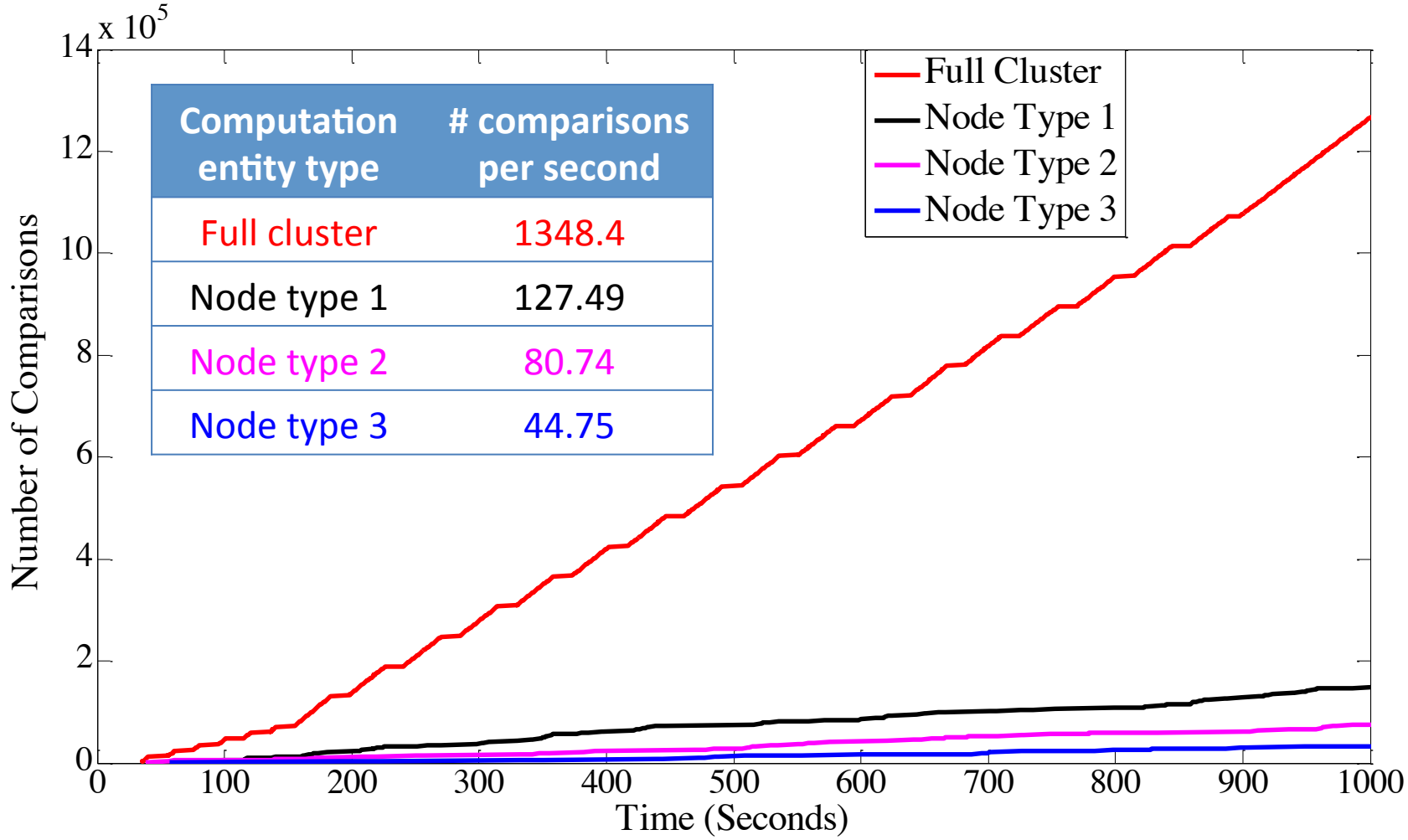


--Best LBP parameters (P,R) are found through experimentation.

--Use of cancelable templates does not noticeably degrade the matching performance

Computational performance

Computation entity type	# comparisons per second
Full cluster	1348.4
Node type 1	127.49
Node type 2	80.74
Node type 3	44.75



Security assessment

- A single key is used to create the cancelable templates.
  - The key is kept secure by generating a hash value using bcrypt.
  - The key cannot be derived from the templates.
- Vulnerabilities if key is compromised
  - If the key is known, the native template could be derived.
  - However, original picture gallery is not compromised.
  - The key should be periodically changed to prevent its compromise.
- Steps to take if templates are compromised.
  - Just need to change the key and generate new templates.
- Matched images stored in user's cache.
  - Should be periodically cleared and/or encrypted.

Outline

1. Introduction
2. Homomorphic LBP-based face recognition
3. A framework for secure cloud biometrics
4. System analysis
5. **Conclusion**

Conclusion and Observations

- By leveraging cloud services, biometric operations can be parallelized to improve the system performance computationally.
- Secure storage of massive biometric data on the cloud is possible using biometric template protection techniques.
  - An approach for generating cancelable templates allows templates to be fully revocable with negligible loss on matching accuracy.
- Multiple mobile devices can be supported by interfacing through a mobile-friendly web application

Future work

- Address scalability issues.
- Formulate key-management and access policies.
- Reduce latency through improved implementation.
- Integrate improved identification algorithms.
- Extend to other modes and other applications.

Thank you for your attention.

Questions?

References

[3] E.Kohlwey, A.Sussman, J.Trost, and A.Maurer,"Leveraging the cloud for big data biometrics: Meeting the performance requirements of the next generation biometric systems," in *Proc. IEEE World Congress on Services*, (Los Alamitos, CA, USA), pp. 597–601, Jul. 2011.

[7] J. Yang, N. Xiong, A. V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie, and Y. Yang, "A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications," *IEEE Systems Journal*, vol. 5, pp. 574–583, Dec. 2011.

[10] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in *Proc. IEEE INFOCOM*, pp. 2652–2660, Apr. 2013.

[12] I. A. Rassan and H. AlShaher, "Securing mobile cloud using finger print authentication," *International Journal of Network Security & Its Applications*, vol. 5, Nov. 2013.