# Privacy Preserving Biometrics based Remote Authentication Protocol for Mobile Devices

March 22, 2016

## 1 Motivation:

There has been a major shift from traditional passwords based authentication to biometrics based authentication in consumer applications in the recent past as major service providers such as the leaders in banking [1, 2, 3], credit cards [4] and e-commerce [5, 6] are adopting biometrics to authenticate users. Biometrics is a strong factor of authentication due to its ability to uniquely identify an individual. Different vendors have adopted it for different motivations, for examples, Amazon uses selfies based on facial recognition techniques to avoid the difficulty in typing passwords to authenticate transactions in mobile devices with small screens [5] and Master cards has adopted it in order to drastically cut-down the cost of false decilned transactions [4].
Two main contexts in which biometrics is being used for authentication are: in-person authentication [7] and remote authentication [2]. In the first case, user is present at the authenticator's premise when authentication is performed and a device of the autheticator captures the biometrics. In the second case, authentication is performed over the network and the biometrics is captured by the user's device. While there are common challenges w.r.t both cases due to the sensitivity (being tightly coupled with one's identity) non-repeatability (no two biometrics samples of the same individual match exactly) and non-revocable (inability to cancel/renew) nature of biometrics, the second case involves more challenges than the first one in terms of liveliness verification of the biometrics to avoid spoofing attacks, secure transmission of the authentication information and security of the user's device. Furthermore, remote biometrics based authentication is being widely used since online-banking and e-commerce applications are increasingly adopting it.
Aforementioned commercial authentication systems that are being deplyoed today, inherit key security concerns irrespective of the fact that they incorporate state-of-the-art facial/voice recognition algorithms and liveliness verification techniques. First, since users' biometrics templates are stored in the server databases for matching during the authentication, they become major targets of attackers. For examples, in Google Hands Free system [7], user's picture taken at the authentication time is matched with the user's Hands Free profile picture and in Citi bank system, user's pre-recorded voice samples are matched with the voice captured when the user call in. Second, multiple third party service providers are storing different biometrics traits of the same user (such as face, voice and fingerprint) for their proprietaty authentication protocols. This creates multiple points of vulnerability on one's biometrics identity, due to linkability [8]. Third, the current protocols require the users to send a raw biometrics sample over the network each time the user remotely authenticates using biometrics, which is not desirable. Stolen biometrics templates from the server databases or from the authentication channels lead to identity theft which poses severe threat to user's digital identity, compared to the case in which a password is stolen, because biometrics samples reveal sensitive features of the user's biometrics identity which can not be revoked.
Therefore, it is best to avoid storing or transmitting sensitive biometrics information during authentication because we can not solely rely on encryption to protect biometrics databases and authentication channels as there have been many instances of password breaches in the past, although such techniques were used to secure passwords during storage and transmission. The second issue mentioned above can be avoided by getting a trusted identity provider (IDP) to enroll user's biometrics identity [7, 9]. However, if the IDP is involved in each transaction that the user authenticates, it undermines the user's privacy since the IDP gets to know about different transactions that the user performs with different service providers.
To address aforementioned security and privacy concerns, we aim to develop a biometrics based remote authentication protocol with following characteristics:

1. User's biometrics identity is enrolled with only a trusted IDP (i.e: biometrics is not stored with multiple service providers).

2. Sensitive features of user's biometrics is not stored anywhere.
3. Sensitive features of user's biometrics is not revealed during authentication.
4. After the initial enrollment with the IDP, users can carry out biometrics based authentication with multiple service providers without involving the IDP. (i.e: user centric authentication protocol as opposed to traditional IDP-centric authentication protocol).
5. Efficient in terms of computation and communication in order for it to be carried out from user's mobile devices.

In what follows we describe our roadmap of realizing the goal of developing a privacy preserving biometrics based remote authentication protocol with the aforementioned characteristics.

# 2 Past and on-going research work:

### 1.1 Overview of the solution:

# 3 Next research goal:

### 2.1 Related work:

### 2.2 Challenges:

### 2.3 Contribution of this work:

# 4 Background and potential impact:

# References


[1] B. Yurcan. (2016) Banks embrace biometrics, but will customers? [Online]. Available: http://www.americanbanker.com/news/bank-technology/banks-embrace-biometrics-but-will-customers-1078867-1.html

[2] N. Cappella. (2016, Feb.) Hsbc announces biometric banking with voice and fingerprints. [Online]. Available: https://thestack.com/world/2016/02/19/hsbc-voice-biometric-online-banking/

[3] P. Crosman. (2015, Feb.) Biometric tipping point: Usaa deploys face, voice recognition. [Online]. Available: http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html

[4] A. MacGregor. (2016, Feb.) Security in rich internet applications. [Online]. Available: https://thestack.com/iot/2016/02/22/mastercard-rolls-out-selfie-verification-for-mobile-payments/

[5] A. MacGregor. (2016) Amazon wants to replace passwords with selfies and videos. [Online]. Available: https://thestack.com/security/2016/03/15/amazon-wants-to-replace-passwords-with-selfies-and-videos/

[6] M. Anderson. (2015) Alibaba demonstrates facial recognition payment system at cebit. [Online]. Available: https://thestack.com/security/2015/03/16/alibaba-demonstrates-facial-recognition-payment-system-at-cebit/

[7] M. Anderson. (2016) Google testing facial recognition payments on android and ios in san francisco. [Online]. Available: https://thestack.com/cloud/2016/03/03/google-hands-free-facial-recognition-trial-san-francisco/

[8] E. B. H. Gunasinghe, "Rahasnym: Protecting against linkability in the digital identity ecosystem," in *The 35th IEEE International Conference on Distributed Computing Systems*. IEEE, June 2015.

[9] "IdentityX | World-Class Mobile Biometric Authentication," http://www.identityx.com.