Security and Privacy Implications of Biometric Authentication: a Survey

D. S. Wijenayake[a,1]

[a]*Department of Computer Systems Engineering, University of Kelaniya, Sri Lanka*

In today's world, biometric authentication is used by a wide range of gadgets and systems to verify user identification and access control. Even though biometric authentication is more secure when compared to traditional authentication methods, it itself is not completely hack–proof as any technology can always be hacked and exposed. Protecting user biometric data is a key security challenge in this field. In case a hacker steals any biometric information such as fingerprints, voice waves, etc. from a user, the hacker can effortlessly access all the systems that the original user has access to, which is a serious security concern. Biometric information is unique and it is even impossible to change as passwords, to block someone using it. This is the most vital drawback of biometric authentication. Therefore, the aims of this paper, are to find, understand and propose remedies to the security and privacy shortcomings of the latest biometric authentication methods. The outcome of the critical evaluation taken place in this research, results that several limitations are there in the recent researches. The lack of generalizations (testbeds and participants of the studies were limited to selected geographical areas when compared to the whole populations of the testbeds/users of the world), fewer experiments, and lack of usability/privacy requirements are among them. The paper suggests solutions/future research directions for the many of aforementioned limitations, such as, implementing indicators which depict the strength of biometric authentication methods' security, rehashing of the studies with different populations via the internet, improving current research-based biometric authentication applications to support multimodal (using of two or more biometrics to authenticate)/continuous authentication, ensuring trust and privacy of users, etc. In conclusion, with the competition among major players in the electronic device market, research-based biometric authentication methods will be rapidly implemented in the real world. To ensure the protection of sensitive data, mobile interfaces should be improved, researchers are highly encouraged to reproduce and critically evaluate others' researches, and the security and privacy of biometric authentication should be maintained without compromising usability. Then only it would be a challenge to hackers to exploit the biometrics.

Keywords: Security and Privacy; Biometric authentication; Multimodal authentication

[1] Corresponding author: D.S. Wijenayake; Tel.: +94-70-274-0836
E-mail address: dswijenayake20360@gmail.com