Biometrics in Security: Ethical Implications and Privacy Risks

Yazed AlKhalaf*, Khaled AlAnbar†

*Al Yamamah University, *202211123@yu.edu.sa*
†Al Yamamah University, *202211365@yu.edu.sa*

I. Introduction

Biometrics have recently become a way to authenticate humans before giving them access to their accounts. NIST defines **Biometrics** as: "A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics." [1]. Its ease of use, and high security make developers confident when putting them in. If that is the case, then we have a few challenges we have to address, mostly on the ethical and privacy sides. Of course things aren't plain white and plain black, there is always the area in between, the grey area in which most of the discussions happen. The Ethical Implications section discusses whether it is okay to keep those records or use them for other purposes without the consent of their users. The Privacy Risks section dicusses which data is considered private and which is public and proves your identity, and if all of the data is private then how to make sure users know what they are getting into.

II. Ethical Implications

III. Privacy Risks

IV. Conclusion

References

[1] National Institute of Standards and Technology (NIST). (2024) Biometrics - glossary — csrc. Definition: A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. [Online]. Available: https://csrc.nist.gov/glossary/term/biometrics