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

Using the biometric data collected from users for purposes other than the reason they have been collected for is unethical. But who decides what is ethical and unethical? The answer to this question depends on which view you use to view the case, but for us as Muslims, we believe in the deontological view only, that is, an action is wrong even if the outcome is good, and an action is good even if the outcome might not seem good if looked in isolation. Our beleif is that Allah is the one who decides what is ethical and what is not, because people can't decide if something is ethical or not, we are all the same, and everyone would choose what suits him or her better. An example of this is whether killing someone because they killed is ethical or unethical. People of the killer might claim it is unethical to kill someone, so why kill our son? But he killed someone, so they are basically having a double-standard. Well, in Islam if someone kills someone they are beheaded with a sword unless the people who have the right of the killed person forgive in return of "Deyya", aka money. So basically Allah is the one who decides which actions are good, "ethical", and which actions are bad, "unethical".

Keeping the context above in mind, it is unethical to keep the biometric data of users for any purpose other than what they have been collected for. Keeping it is basically stealing the data, and that is unethical. But let us say a bad actor keeps the data and doesn't follow the guidelines, what are the implications? First of all, if the data is leaked, the user's identity can be stolen online if a website only uses biometrics and they are cloned. The data also can be sold in the black market, identity theft but with the biometrics of a human being!

III. Privacy Risks

Identification through biometrics has become common, yet it comes with a major drawback, and that is often privacy loss. When comparing biometrics data like fingerprints, facial or voice and conventional identification data like passwords or PINs, biometric data is strong and personal (one of one), which makes it nearly impossible to replicate or even fabricate it. Even though it is hard to be fooled this are some privacy risks according to Maurice Uenuma: "Data theft, Spoofing and impersonation, Privacy concerns, and Integration challenges " [2].

Starting with data theft, "Stolen biometric data can lead to unauthorized access to enterprise systems and theft of sensitive information" [2]. When discussing unauthorized access or data theft, you're addressing the primary privacy risk, which is why i began with it initially. This attack occurs when an individual gains access to the data either during transmission or by retrieving it from its storage location, such as a computer database.

Secondly with spoofing and impersonation, "Biometric systems can be tricked using various spoofing techniques, such as fake fingerprints, facial images, or voice recordings" [2].

Thirdly with privacy concerns, "Collecting and storing biometric data raises privacy concerns, as individuals may worry about the misuse of or unauthorized access to their personal information" [2]. Due to technological advancements, it is increasingly difficult to keep personal data private. Personal information includes everything from a person's name to their IP address to their face. For instance, on Facebook, you can typically search for a person's name and gain access to all their personal information.

Lastly with Integration challenges, "Poorly integrated biometric systems may introduce vulnerabilities, especially when integrated with other security or IT systems* [2]. By providing the precise details required for authorization, integration aims to enhance security. However, achieving this can be challenging due to factors such as image quality, environmental conditions, and system limitations.

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

[2] D. Reading, "Navigating biometric data security risks in the digital age," Nov 2024, accessed: 2024-11-23. [Online]. Available: https://www.darkreading.com/cyber-risk/navigating-biometric-data-security-risks-digital-age