CYSE 425W Policy Analysis: Ethical Concerns Regarding the use of Biometrics

Alysia Beckles

Old Dominion University

CYSE 425W Policy Analysis: Ethical Concerns Regarding the use of Biometrics

**Introduction**

 People have been heavily reliant on technology. As technological innovations have become prevalent in people's lifestyles, from home appliances to mobile phones, it enhances functionality and provides efficiency. A benefit of technological innovations is that it enables users to store and access their sensitive data efficiently. While availability and integrity became an improvement for people, security measures to shield them are implemented through technological innovations. It can give people the ability to gain physical or digital entry to places too. There will be some positives and negatives when using technology. Biometric technology is meant to provide users extra security that prevents threat agents from having unauthorized access to users' sensitive information and organizations. Although biometric technology is meant to deter threat agents from gaining entry to users' confidential information and organizations’ assets easily, technological advancement has created concerns. In the financial industry, many financial institutions had made strides towards implementing their services virtually and are encountering issues with biometric technology.

**What are Biometrics?**

Biometric technology is an identification and verification process. It is a measurement of users’ physical features. Biometric technology will scan several parts of their phenotypes, from fingerprints to facial features, such as eye recognition. It can extend to a multitude of physical attributes such as voice recognition, DNA matching, etc. This type of technology enables companies to implement a method to manage entry to the organization and its systems (Bustard et al., 2014, p.55-56). Fingerprint security is used by most financial institutions today when users utilize their virtual services since there is an agreement by most that it is convenient and cost-effective in the financial industry (Nagaraju & Parthiban, 2015, p.5). For instance, a sensor will record the user's biometric data, such as their fingerprints, and the financial institution will collect the data. When a user wants to monitor or modify their banking information remotely, they are required to utilize their fingerprints as a method to access their device. As a result, this will try to discourage another user from placing their finger on the company's sensor and obtaining entrance.

**Weaknesses Perpetuated by Biometric Technology in Financial Institutions**

Some institutions believe that incorporating biometric technology will thwart unauthorized threat agents from obtaining or modifying their sensitive financial information and sell it to others for nefarious reasons (Venkatraman & Delpachitra, 2008, p. 415). Maintaining the confidentiality, integrity, and availability of financial information is an important function of these types of institutions. Issues emerge because the technologies utilize information from the observable features of users. Using this type of technology will become a problem since that data could be impacted by threat agents that can manipulate and replicate it.

Many financial institutions will store the biometric data in a centralized system from users who utilize their virtual services, which leads to security and privacy issues (Venkatraman & Delpachitra, 2008, p.420-424). It will be difficult to store biometric data safely since the hashing method utilized to safeguard passwords will not work. Comparably, biometric technology requires high-level security to maintain (Patwary et al., 2021, p.23). Threat agents such as hackers will be able to gather financial information from those who use their virtual banking services through sophisticated techniques and cyber-attacks that target biometric technology. As they expand their knowledge of biometric technology security protocols, threat agents are starting to learn how to exploit exposures in biometric scanning software to gain entry and share information on how to circumnavigate these susceptible systems. Hackers can easily infiltrate a financial institution's database that is breached and unprotected by utilizing techniques such as exploiting URL searches to gain access to critical information. Then, they will have the ability to collect biometric data such as their fingerprints and use it since that type of data cannot be altered, fingerprints will remain the same (Taylor, 2019).

There is software and hardware available for those who want to utilize biometric data to gain access too. There is software available for those who want to utilize biometric data to gain access too. For instance, VeriFinger software is a tool that will reconstruct an individual's fingerprint from a photo of somebody's thumbprint (Howell, 2017). Also, some threat agents do not have to be an expert in exploiting systems since biometric data is public. They can easily record a person's voice if voice recognition is necessary for entry. Presentation attacks enable threat agents to mimic users who have enrolled in the virtual banking system of their financial institution by utilizing an artifact too. For instance, the threat agent will seize the registered user's fingerprint, and an identical fingerprint will be created (*How biometrics are attacked*, 2019). A threat agent can interrupt the data output, and the biometric data collected can be replaced by the attacker's or another individual. Biometric technology is also susceptible to denial-of-service attacks too, making it difficult for users to access their financial information virtually (*How biometrics are attacked*, 2019).

**Conclusion**

Thus, biometric technology has a variety of disadvantages. Implementing this is meant to be an alternative to a personal identification number or a standard password. Threat agents are continuously trying to bypass biometric systems as the technology progresses with more advanced approaches. Although biometric technology is the type of security measure adopted by many financial institutions, it has developed flaws by disregarding security and privacy.

**References**

Bustard, J. D., Carter, J. N., Nixon, M. S., & Hadid, A. (2014). Measuring and mitigating targeted biometric impersonation. *IET Biometrics*, *3*(2), 55–61. https://doi.org/10.1049/iet-bmt.2013.0054

*How biometrics are attacked*. NCSC. (2019, January 24). Retrieved October 14, 2022, from https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked

Howell, K. (2017, August 28). *3 problems with biometric security, including fingerprint ID*. Ipswitch. Retrieved October 14, 2022, from <https://www.ipswitch.com/blog/3-reasons-biometrics-are-not-secure>

Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and Privacy Protection Gateway. *Journal of Cloud Computing*, *4*(1), 5–23. https://doi.org/10.1186/s13677-015-0046-4

Patwary, A. A.-N., Naha, R. K., Garg, S., Battula, S. K., Patwary, M. A., Aghasian, E., Amin, M. B., Mahanti, A., & Gong, M. (2021). Towards secure fog computing: A survey on trust management, privacy, authentication, Threats and Access Control. *Electronics*, *10*(10), 1–52. https://doi.org/10.3390/electronics10101171

Taylor, J. (2019, August 14). *Major breach found in biometrics system used by banks, UK police and defence firms*. The Guardian. Retrieved October 14, 2022, from <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information Management & Computer Security*, *16*(4), 415–430. https://doi.org/10.1108/09685220810908813