Analytical Approach to Biometric Security and How It Affects Privacy

Torré A. Williams, twill049@odu.edu
Center for Cybersecurity Education and Research
Old Dominion University

Kazi A. Islam, kisla001@odu.edu
Research Assistant Professor
Old Dominion University

Submitted in partial fulfillment of the requirements with the
COVA CCI Undergraduate Research Project

December 2021

I. Abstract

In this time where the world is using technology every day, there is going to be a need for some type of security to take place to protect its citizens from unwanted harm or danger. The use of any authentication methods is becoming very essential for a lot of companies and even for your own personal belongings. The use of biometric technology has offered companies the chance to upgrade their security system. This has also provided easier ways that people authenticate themselves as who they say they are. Due to their growth of usage, there is a privacy and security concern of these biometric data. In this research, we developed an analytical approach to biometric security in relation to privacy. This research will focus on the history, current state, problems/concerns, and the future development of biometric security. Biometric will be a forever growing topic and forever changing as time goes by. There will be a future in how companies will be using biometric technologies to better secure their systems.

II. Introduction

Why is authentication important? Authentication is considered one of the most important human interaction components with a computer. It verifies any user that has access to the computer to make sure the user is who they say they are. However, the use of biometric security systems offers a more reliant and efficient way of better authenticating a person's identity. With biometric technologies, it is much harder for someone to fake their identity (Phadke, 2013). Biometric technology is designed to link a physical characteristic to that individual, that is supposed to be different from everyone else (Phadke, 2013). The use of biometric systems is operated in two forms of security access- verification and

identification. Verification confirms and verifies a user. The user is to provide some sort of identification that is either recognizable or dismissed by the system. In the approach of identification, the system determines the identity of the user and says who they are. According to Clark (2015), most businesses and organizations are trying to attempt every aspect of biometric technologies to increase their security measures within their business. As technology is constantly growing to fit our everyday lives, no matter how far biometric technology may grow, there will always be concerns that will be directly towards privacy and to whom this data is being shared with. Along with growing our technology, there is a level of expectation of privacy that is owed to the public. While thinking of this, the question is "if advantages of technology solely exist to remove barriers to privacy?" "If so, is that something we can live with in exchange for convenience?" (Clark, 2015).

Though there are huge improvements in biometric technology, there are concerns about how accurately it will prevent hackers from committing identity theft, stealing personal data, or any financial loss (Pandya, 2019). These are challenges that companies are constantly facing. With certain features of the biometric technologies, it is not intended to invade people's privacy, but in some cases fraudulent may happen due to the security features biometric technology possess if it is not implemented properly (Pandya, 2019).

III. Background

The word biometric came from a Greek word "bios" meaning life and "metrikos" meaning measure. Scientifically speaking, biometric uses a "biological characteristic" to help identify and recognize an individual. The first use of biometric technology was in the late 1800s in India by Azizul Haque. There he created this system called the Henry system

which was made to identify fingerprints. Still to this day this system is still in use. The most used way of authenticating an individual is the use of passwords. Passwords do indeed add some security measure; however, biometrics adds an additional layer that can safely secure the identity of an individual. The use of biometric technology brings promising security applications for some companies. Biometrics rely on either something you know; for example, a pin or password, or something you have; for example, card or a key. To have a great biometric system, it must have good quality characteristic traits that will make up a good use of biometric. Here are the following: fingerprint, speech recognition, iris, retina, face, signature, hand-geometry, keystroke, or palm-print.

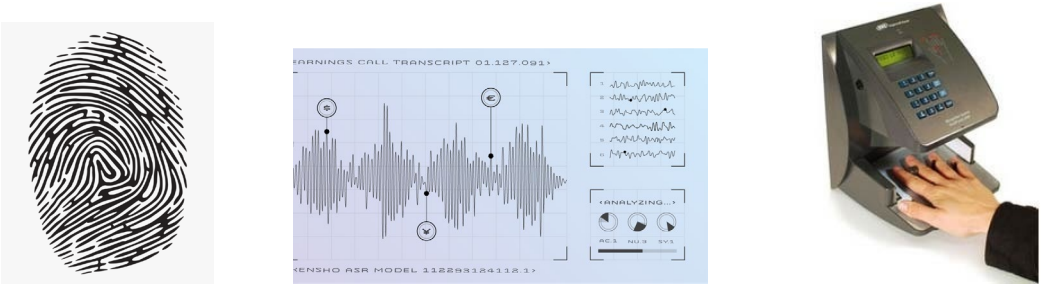

Figure 1. Examples of different forms of biometric traits

The most widely used biometric trait is face recognition. In airport boarding, their technologies are finding a way to upgrade their systems using a contactless facial recognition measure for all their passengers. Since COVID-19 has been going on for a while, airports have been trying to figure out how to safely make boarding with as little contact as possible. With facial recognition, this software can locate and identify dozens of features about a person's face, which will allow them to be able to access certain facilities in the airport. Examples, like using their face to be able to access and use it as their own boarding pass (Youd, 2021).

There is a threat towards privacy that biometrics bring. It doesn't come from the correct use of biometric technology; it comes from when there is a third-party accessing information without any consent. Some companies all over the world are carefully adopting it or discarding this technology at all for the sake of keeping the people's privacy.

IV. Privacy concerns

Operating on computer systems, it is very crucial to implement the proper use of authentication and identification. To remain a high level of privacy, some may feel that there is a need to stay away from anything that evolves being on the internet. However, if there is a need to be up there like dealing with credit card payments, traveling, mobile phones, or any financial institution, etc... then there is a certain level of privacy that is given up. One of the biggest problems surrounding privacy is the use of monitoring and surveillance systems by government officials, which lack the capacity of providing "legal protection". Though biometric technology brings a great deal of security, there are ways that companies can implement it without disrupting the privacy of individuals. Understanding what is expected, the root of understanding how it will affect biometrics among programs used by the government- all this can be traced back by understanding privacy written in the Fourteenth Amendment under the Due Process Clause (Woodward, 2003). There are three distinct areas that the courts have categorized what realm of privacy government are forbidden to enter. Physical privacy, decisional privacy, and informational privacy- these are the three distinct forms. Physical privacy has the greatest protection considering the fourth amendment against unreasonable searches and seizures with law enforcement. Decisional privacy allows individuals to make his or her own decisions about

their intimate and personal matters that may affect their lives without the interference of government officials. For example, marriage, family relationships, or education. Informational privacy allows individuals to be able to control how, when, and to what extent information about them is open and shared with others. The amount of information that is required from citizens that is being used by the government to gather enough information for storage, dissemination, and use in their databases brings a lot of concerns dealing with physical and informational privacy. There is a juggle for businesses to be able to enhance their security measures by implementing biometric security without interrupting privacy concerns from the public. The more the people are hesitant about privacy concerns, businesses are more than likely to pass up the adoption of biometric technology. (Clark, 2015).

The use of biometric technology has always been a concern for many organizations. It has not always been the go-to move that people wanted to associate their company with. Some viewed biometric as it increases criminal activities by using fingerprints to identify an individual. Law enforcements have been using fingerprints as means of identifying a possible criminal but using it has brought many questions on what a major loss of privacy and dignity that it brings. The idea of using biometric technology is to not only enhance security by authentication but to protect certain images that may be "unique" to link it to identifying a person. Also, other information like accidentally obtaining a person's medical history which may bring concerns on how well this system is adhering to privacy rights. For example, New York has implemented a biometric privacy law that is supposed to maintain privacy among customers with use of biometric technology. This law is

specifically designed for businesses to follow, and if they don't adhere to these conditions, they will suffer a large penalty. Businesses that use biometric technologies are to warn customers at the door about what information is being collected and how it will be collected, so that everyone is on the same page. (Whittaker, 2021). This law doesn't give stores, retailers, or restaurants, etc... the permission to be able to sell or profit from any data that they collect. Other states like Oregon and Illinois, etc... have passed similar laws regarding the privacy act against biometric technology. Law named the "Biometric Information Privacy Act", this law allows citizens to be able to sue any company for using their biometric information without any consent (Whittaker, 2021).

V. Current state of biometric

As technology is growing at a steady paste, the use of biometric systems and how it's being used is bringing privacy concerns at large. These issues are becoming more and more frequent among users. On the other hand, the increasing level of using biometric technology to quickly identify a person can potentially lead to illegal activity, like spying. To prevent this from happening, there needs to be safety measures that still protect people's anonymity at a certain level. Currently in this age of technology, fingerprint and face recognition is currently being widely used the most out of all the biometric traits.

With the current trends of cybersecurity issues, like terrorism, identity theft, and fraud; these issues brought up the development of biometric solutions that are being implemented today. Here are a few areas where biometric security solutions are being used (Google, 2015).

- Law enforcement: Law enforcement uses a type of system called Automatic Fingerprint Identification Systems (AFIS). This system searches, retrieves, and stores fingerprint images and any other records on an individual. Another type of system that is used within law enforcement to help with any type of imaging or facial recognition is the AwareABIS. This system is based on a Biometric Service Platform (BioSM^{TM}). This system provides a more advanced way in how biometric data is processed and managed (Google, 2021).
- Military: Since 2009, the military has been incorporating the use of a biometric program that has been able to help them identify non-U.S. citizens that were on the battlefield. The biometric system is authorized and monitored by the Defense Forensics and Biometrics Agency (DFBA). Using this database, it has been a game changer for the military and how they operate. “Forensics and biometric are the foundation capabilities that allow us to identify individuals and verify a claimed identity with certainty” (Thomas, 2021).
- Healthcare and subsidies: To confirm the identity of an individual, they use biometric ID cards to verify their identity to access any governmental healthcare and services.
- Automotive: Companies like Mercedes and Volkswagen are jumping on board with implementing biometric technologies within their car’s system. Face recognition and smart sensors, that recognize gender, height, and other identifiable factors to be able to identify an individual.
- Mobile devices: With Apple iPhone, the phones have implemented security measures as well as fingerprint scanners and facial recognition. Not only have

mobile devices have implemented biometric technology but laptops and video devices have as well included scanners and voice recognition.

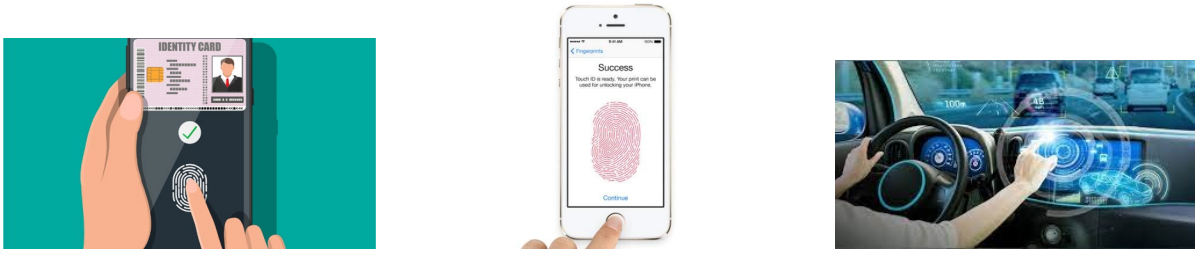

Figure 2. Examples of different forms of biometric technologies

VI. Future and Alternative of biometric

Many bring up the question on how to prevent the use of biometric authentication from becoming such a large avenue for many corporations when it comes to our privacy?

In this time where covid is still around, the “traditional” use of biometric has been a struggle and has not worked to the best of its ability within the last year. Because gloves and masks have made it harder for biometric technology to read and verify the user, some believe that the use of behavioral biometric could be what is going to rise in the future. Every human being is given a unique characteristic that makes them who they are, so why incorporate behavioral biometric in the mix. Everyone behaves differently and everyone has their own way of doing things. Whether that be habits or how everyone acts, there is no one that can come close to having the same characteristic traits. Creating a model for the different behaviors that people have and compare it to see if it matches up with a person claiming who they say they are.

Areas in which behavior biometrics can make a difference in people’s lives. Physical access can allow your home, car, or office to be unlocked with a single movement as the user comes close enough to open it. If there is a personal phone nearby.

VII. Conclusion

To maintain a high level of biometric security, any company should incorporate a variety of different security measures and techniques. As I mentioned earlier in this paper, the use of biometric technology allows us to authenticate and verify a person based on the characteristics that are uniquely connected to them easily and uniquely. Adopting this use process will help monitor the number of times users are signing in to make sure there is no one trying to access something, that they have no business accessing. We continue to live every day, the concept of what is private and what we as society think privacy will eventually change. Any business or organization that is using biometric technology will have to keep up with having the best security protocols like encryption, that will restrict the authentication of biometric data. Along with the use of biometric technology, it is said that the company must inform its clients and employees of the expected loss of privacy that may come with being involved with their company. By doing this, at least it gives clients and employees a choice to whether they want to move forward with this company.

VIII. Reference page

Cavoukian, A. (1999). *Privacy and biometrics*. Information and Privacy Commissioner/Ontario. **https://www.ipc.on.ca/wp-content/uploads/Resources/pri-biom.pdf**

Memon, N. (2017). How biometric authentication poses new challenges to our security and privacy [in the spotlight]. *IEEE Signal Processing Magazine*, *34*(4), 196-194. **https://ieeexplore.ieee.org/abstract/document/7974880**

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, *21*(6), 15-26. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1662038

Pinto, J. R., Cardoso, J. S., & Lourenço, A. (2018). Evolution, current challenges, and future possibilities in ECG biometrics. IEEE Access, 6, 34746-34776. https://ieeexplore.ieee.org/abstract/document/8392675

Rhodes, K. A. (2003). *Information Security: Challenges in Using Biometrics*. General Accounting Office. https://www.gao.gov/assets/gao-03-1137t.pdf

Crowley, M. G. (2006, December 5). *Cyber crime and biometric authentication – the problem of ...* Retrieved November 15, 2021, from https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1069&context=ism.

Clark, B., & Bryan Clark (67 Articles Published) . (2015, March 5). *The history of biometric security, and how it's being used today*. MUO. Retrieved November 15, 2021, from https://www.makeuseof.com/tag/the-history-of-biometric-security-and-how-its-being-used-today/.

Youd, F. (2021, July 2). *Contactless Airport Boarding: Biometric technology with Sita*. Airport Technology. Retrieved November 15, 2021, from https://www.airport-technology.com/features/contactless-airport-boarding-biometric-technology-with-sita/#:~:text=Technological%20advances%20have%20seen%20biometrics,access%20facilities%20around%20the%20airport.

Google. *Biometrics: Definition, use cases, latest news*. Thales Group. (2021, June 2). Retrieved November 15, 2021, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

Phadke, S. (2013). *(PDF) the importance of a biometric authentication system*. Retrieved November 22, 2021, from https://www.researchgate.net/publication/266967332_The_Importance_of_a_Biometric_Authentication_System.

Pandya, J. (2019, April 17). *Hacking our identity: The emerging threats from biometric technology*. Forbes. Retrieved November 22, 2021, from https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/?sh=1ae939295682.

Thomas, D. A., Solutions, B. R. T. R. C. F., & Dfba. (2021). *Defense Forensics & Biometrics Agency*. DFBA. Retrieved November 22, 2021, from https://www.dfba.mil/.

Whittaker, Z. (2021, July 9). *New York City's new biometrics privacy law takes effect*. TechCrunch. Retrieved November 22, 2021, from https://techcrunch.com/2021/07/09/new-york-city-biometrics-law/.

Woodward Jr, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition*. RAND CORP SANTA MONICA CA. https://apps.dtic.mil/sti/pdfs/ADA414520.pdf