Biometric Usage and Risks Across Different Age Groups

Ayanna Armstrong
Computer Science Department
Hampton University
Hampton, VA

Abstract- This report will discuss biometric usage and its risks across different age groups in a time when biometric technologies continue to grow. This report will also discuss how different age groups utilize biometric systems, the advantages and disadvantages of these systems, and the affect it has on the identified population. Issues on biometrics on an ageing population will also be touched upon. This study utilizes surveys conducted to identify and compare the different ways the population uses biometrics and identify the risk associated with distinct usage.

I. Introduction

You are your own key. Biometrics, which are based on this simple idea, have become a popular alternative to traditional identification systems such as tokens and passwords. Biometrics was once confined to science fiction, but in the last decade, we have witnessed the emergence of biometrics in our daily lives. In recent years, biometric technology has advanced quickly. It is now uncommon for us to not encounter some form of biometric technology. Everything from unlocking your phone to checking the weather for the day to safely boarding a flight is covered. Biometric technology pervades our daily lives.

A. Problem Statement

With the increased growth of biometric technologies, it is expected for the population to take use of the advancements. The younger population relies on biometric technology for almost everything, while the older population doesn't use at as often and in the same ways. It is imperative that users of biometric technologies are aware and proactive towards protecting their cyber-identity as well as data the associated.

II. Methodology

This study will use a combination of a literature review and a user survey to collect data and gather results directly related to my thesis. The survey will be comprised of the participant declaring their age to be put into the correct age group. They will then go on to explain in what ways they use biometric technology along with any security risks they experienced. I will also be looking at what risks are associated. Analysis of these components along with comparisons and differences will create a very clear understanding of the essays matter.

A. Literature Review

I will discuss the use of biometric technologies and how the population utilizes them. I will then go into detail on the advantages and disadvantages of biometric systems for the population outside of business use. Through this literature review, details about how often the different population groups (young people and older people) use these biometric systems and in what ways. With this, I can compare the research that has been done around the topic and the actual proof from the survey I conducted.

The use of biometric can be dated back to the 1860s. Morse code telegraph operators recognized one other by the manner they sent dash and dot signals. Allied troops used the same method to identify senders and authentication messages they received during World War II. The primary premise of biometric systems is to identify a person based on their unique traits.

Fingerprint recognition is one of the first and most well-known biometric technology that has been lumped together under the umbrella of digital forensics [11]. With the proliferation of video surveillance cameras in major cities, the usage of the data gathered by these cameras has become a lightning rod for privacy and human rights concerns. Following the terrorist attacks of September 11, 2001, the use of facial recognition as a means of detecting potential threats, particularly in crowded locations, has been widely explored. The technology operates in a straightforward manner. CCTV cameras in streets, public spaces, and business buildings record images 24 hours a day, seven days a week, and sophisticated algorithms compare the images to a database of prospective "villains" or "targets." A match will result in increased surveillance and the possibility of future and additional action. The matching database should be as large and comprehensive as feasible for the system to be effective. It's unsurprising that, to build such a database, security agencies never consult or ask permission to keep people's records in their data centers (at least, I haven't found any proof of this). Furthermore, habitual phishing efforts via the Internet and social networks provide fertile ground for not only a one-dimensional set of data (pictures and other personal data),

but possibly three-dimensional datasets of associated friends, links, habits, and, in many cases, present location.

Furthermore, billions of dollars are being invested in the development of various biometric technologies capable of identifying anyone anywhere in the globe, according to a US Homeland Security newswire. Iris-scanning and foot-scanning technology, as well as speech pattern ID and facial recognition technologies, are among them.

When biometric data is originally recorded and when it is altered, it is also highly vulnerable. Data is at risk during these moments because it can be tampered with from a single point of interaction. During the sign-up process for biometric enrolment events, the biometric system may be vulnerable to fraud. It is critical to confirm identity during the enrolling process, or the entire system will be hacked. Familiar fraud is similar in that it occurs during enrollment or a change to the data that has been recorded. In this case, someone "acquainted" with the person being identified takes control of the device used to sign up and records his or her own data rather than the data of the account owner.

The key issue is that biometric authentication methods raise privacy and security concerns, as there is no way to restore the harm once biometric data has been hacked [12]. You can reset a compromised password, but you can't alter a compromised biometric like a fingerprint, ear picture, or iris scan. You can modify the biometric used in some cases, but even those that can be switched are limited. Biometric identifiers explicitly link a person to a system or activity. That's good when using a fingerprint or facial scanner to unlock your phone, but there are other connections that people won't like; for example, when used to authorize card or debit transactions, your purchase history is uniquely linked to you.

There are many reasons why the general population, government, and businesses rely on biometric technologies. Biometric authentication and its uses in modern-day tech and digital applications has several advantages [13]. By authenticating a concrete, real-world attribute as both something the user has and something the user is, biometrics enable additional levels of assurance to providers that a person is real. Most users' passwords, PINs, and personal identifying information have most certainly been exposed because of a data breach, which means that fraudsters with the answers to traditional authentication methods can access billions of accounts. Biometric authentication adds a roadblock for fraudsters that only a real, authorized user can get around - even if a fraudster knows a person uses their dog's name and some lucky numbers for most of their online accounts, they won't be able to use their fingerprint to unlock an account if they can't provide it right away. Furthermore, biometrics can only be provided by real, breathing people; a robot would have a hard time passing an iris scan at this time.

Another reason biometric technologies are used it because biometrics like face patterns, fingerprints, iris scanning, and others are near-impossible to replicate with current technology. There's a one in 64 billion chance that your fingerprint will match up exactly with someone else's [1]. Said a different way, you have a better chance winning the lottery than having the same fingerprint as a hacker trying to get into your account that's secured by biometrics.

Biometric authentication and its use in modern-day tech and digital applications has some drawbacks, despite greater security, efficiency, and convenience. Hackers are constantly threatening businesses and governments that acquire and preserve personal data. Because biometric data is irreplaceable, businesses must treat sensitive biometric data with greater caution and security - a costly and technically demanding task if they are to keep ahead of fraud advances. If a password or pin has been compromised, it is always possible to change it. Physiological and behavioral biometrics, on the other hand, cannot be said in the same way.

As the globe uses more biometric authentication systems, such as facial recognition technology and other biometric security measures, users' privacy must be considered. When biometrics are converted to data and stored, a user bears the risk of leaving a permanent digital trace that might be monitored by malevolent entities, especially in areas or nations with extensive surveillance. Organizations and governments have utilized face recognition software to follow and identify people with frightening accuracy, infringing on people's privacy [3]. Biometric data can become a permanent digital tag that can be used to follow someone, both with and without their knowledge, as surveillance grows.

Bias is another key issue and disadvantage for biometric technologies because providers face a problem in minimizing demographic bias in biometrics when validating applicants' identities during digital onboarding. Discrimination and exclusion can occur as a result of poor technology deployment or malicious misuse. Cross-demographic performance can be unreliable without an established, document-centric identity proofing solution, limiting client access to fundamentals like credit and the growing spectrum of digital services.

Lastly, the idea of false positives and inaccuracy is a threat when it comes to any person utilizing biometric technologies. To confirm a user's identity, many conventional biometric authentication methods rely on partial information. During the enrolling step, for example, a mobile biometric device will scan a whole fingerprint and convert it to data. Future biometric fingerprint authentication, on the other hand, will only use sections of the prints to authenticate identity, making it faster and faster. In 2018, a New York University research team developed an Artificial Intelligence framework that was able to successfully crack fingerprint authentication with a success rate of 20% by matching partial prints to full biometric data [4].

Technical Difficulties, Ethical Issues

The use of biometrics raises several ethical and societal difficulties. These include issues of privacy, data protection, and proportionality. Though of course important, these issues are not our concern here; rather we consider an ethical and societal issue arising specifically from ageing's challenge to biometrics. We suggest that biometrics implicitly labels older people as 'problematic', 'difficult', and 'unusual'. Biometrics 'problematizes' ageing, and in so doing tends to exacerbate

existing issues of social, economic, political, technological, etc. exclusion which older people face.

If older people cannot be enrolled on an identification system, and if that system is linked to provision of important societal goods (e.g., pensions, access to education or banking, etc.), there is clearly a problem of exclusion: older people are excluded from access to those societal goods. However, even when older people are successfully enrolled on a system, the problem of exclusion may still emerge, which may in turn save them from security risks that younger people are more susceptible to.

The way young people engage online is continuing to be shaped by increased exposure to biometric technology. While most people praise the technology for its ease of use, convenience, and performance, stakeholders are voicing legitimate concerns about how it opens up new ways for privacy to be violated in unprecedented ways [14]. Biometric data is simple to hack, and the repercussions of misusing it might be disastrous. At the forefront is how IoT devices and services are increasingly collecting, storing, and transmitting private information on the cloud, leaving them more vulnerable to identity theft.
Biometrics' simplicity and performance, in the end, trump most of the security and privacy threats. We may expect the use of biometrics to grow in the future.

B. User Survey

I will collect data from users of biometric technologies across the different age groups through conducting a survey. The purpose of my survey is to understand what biometric technologies the younger and older population use and how they use them. I will analyze this survey along with other sources of information to find any patterns and make conclusions related to my thesis.

III. Results

This section will cover the cumulative results obtained from my research methodology outlined in Section II.

A. Advantages of Biometrics

One of the primary advantages of biometric authentication is its convenience; by using something that is a part of you rather than a password or PIN that must be remembered, you can quickly gain access, whether to a physical building or an online service [6]. The most significant advantage of biometric technologies is security. Passwords and PINs can be stolen but stealing a biometric identifier such as a fingerprint or iris scan is extremely difficult. [1] Because of this combination of security and convenience, biometric technology adoption will continue to rise in the coming years, and biometric security systems will become more common. The COVID-19 pandemic has also hastened the need for biometric technology. Contactless access to buildings and services, as well as contactless payments and ATM interactions, are more important than ever [5]. Even after we have COVID-19 under control, the pandemic's effects will be felt long after a vaccine has been developed, with a change in the way we all interact, both with other people and with physical contact in general [10].

B. Usage in the Age Groups

Younger people have a more permissive attitude toward their personal data, with 32% of those polled indicating they safeguard all their personal data sources with a single password or PIN [2]. Over 20% of Generation Z members have shared their online banking passwords with others, while 32% have shared their smartphone password [3].By the end of 2025, more than half of 16 to 24-year-olds believe passwords will be obsolete, replaced by verification technologies such as facial recognition, fingerprint, and retina scanners [7].

While older persons are often slower to adopt new technology than the general population, they are indeed a larger proportion of users [15]. In 2019, 91 percent of Americans aged 65 and up had a phone, with 53 percent having a smartphone [4]. Companies are rapidly inventing and marketing mobile technology to older individuals to assist them in aging in place, staying connected with family and friends, and maintaining their independence. Existing technology, such as wearables and personal digital assistants, can also be beneficial to older persons who are trying to maintain their health and live independently.

C. Common Vulnerabilities

Biometrics is a branch of information technology that is quickly evolving. Biometric technologies are computer-assisted methods and systems for identifying people based on their biological and behavioral traits [9]. Biometric technology has several advantages over traditional identifying methods. Countries are examining these advantages and migrating to next generation identification systems based on biometric technology to take necessary safeguards against increasing security dangers in the modern world. Information security systems are increasingly relying on biometric systems as a key component (gateway).

Biometric system vulnerabilities are mostly caused by the system's structure, biometric characteristics employed (e.g., fingerprint, iris, etc.), and administration policies. Each of these sectors has its own set of vulnerabilities that must be investigated before countermeasures can be taken.

Information about biometric system attacks is a major source of vulnerability information. Attacks are described using a method based on the logical structures of biometric systems. Each biometric system is made up of four key components:

- Sensor module: A sensor collects a person's biometric data and converts it to a digital representation.
- Module for extracting features: The input sample is processed, and a compressed image called template is created. A database or a smart card is used to store the template.
- Module for matching: This module compares the biometric sample to the template. Only one matching is conducted in verification mode, resulting in only one matching score, whereas in identification mode, the supplied characteristic is matched with numerous templates, resulting in many matching scores.

- Decision module: Based on the matching score or security threshold, this module approves or rejects the user.

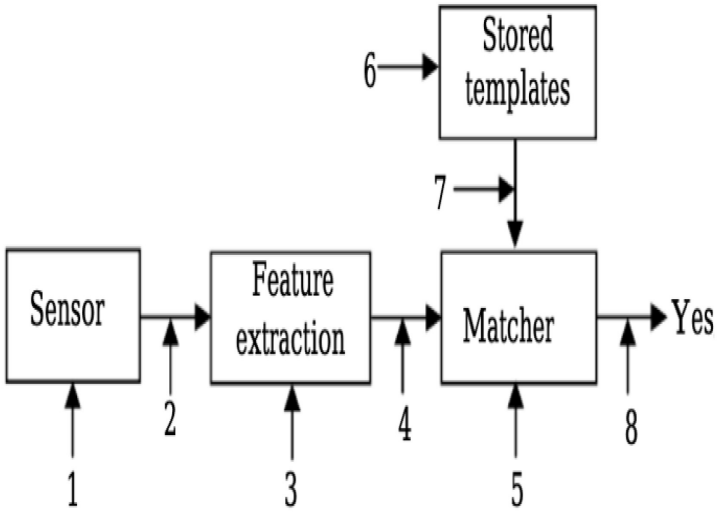


Figure 1: Attack points of a biometric system

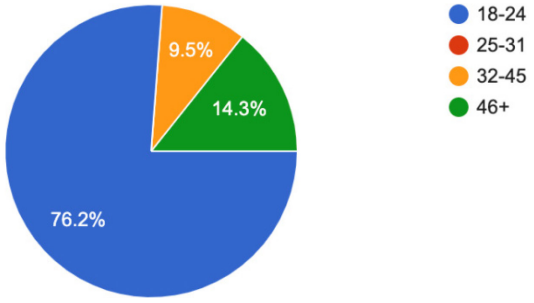
D. Attack points of a biometric system

Characteristics of these attacks are listed and described below:

1. Fake biometric sample presented to the sensor: To gain access to the system, a fake biometric sample such as a fake finger, image of a signature, or a face mask is presented to the sensor.
2. Replay of recorded digital biometric signals: A signal is replayed into the system without considering the sensor. Replaying an old copy of a fingerprint picture or a recorded audio transmission, for example.
3. Denial of feature extraction: Using a Trojan horse attack, the imposter creates a feature set.
4. Spoofing the biometric feature: A bogus set of features replaces the features derived from the input signal.
5. Attacking the matching module: When the matching module is attacked, the matching scores are replaced with bogus ones.
6. Database spoofing: A database of saved templates can be local or remote. One or more biometric templates in the database are faked by the attacker. As a result, either a forged identity is approved, or a legitimate person is denied service.
7. Attacking the communication channel between the template database and the matching module: Stored templates are sent to the matching module via a communication channel. An attacker can alter the data in the channel.
8. Attacking the final decision process: The authentication system function will be overridden if the final decision can be inserted or blocked by the hacker.

E. User Survey Results

I conducted a small survey to analyze how the different age groups use biometric technologies. With the collected data, I could further understand the risks associated. My survey consists of 8 questions, and I had 42 respondents complete the survey. The answers of my survey are anonymous and consisted of people from a variety of age groups and occupations. The findings of my survey are as follows:

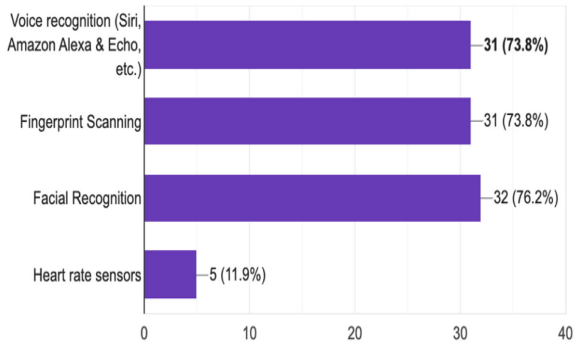


Age Range	Number	Percentage
18-24	32	76.2%
46+	6	14.3%
32-45	4	9.5%

Figure 2: User Survey Age groups

My survey results show that most users are between the ages of 18 and 24. Since most of my respondents are between the ages of 18 and 24, my data and further analysis will be geared to that age group since they stand as the majority.

I prompted the users to select biometric technologies they use. This is the result:

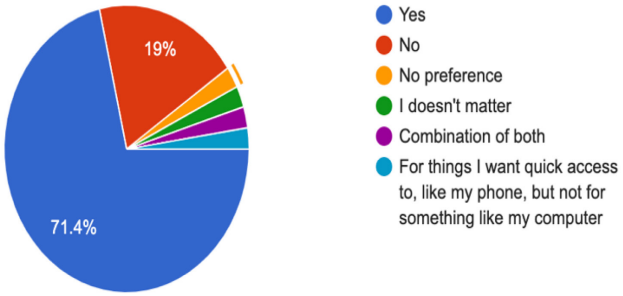


Technology	Number	Percentage
Voice recognition	31	73.8%
Fingerprint Scanning	31	73.8%
Facial Recognition	32	76.2%
Heart Rate Sensor	5	11.9%

Figure 3: User Survey Biometric Technology

From this chart, the most popular form is a tie between facial recognition and voice recognition. This is easy to understand because the newer models of mobile phone and technologies require facial scanning to unlock and utilize Siri, virtual audio guide.

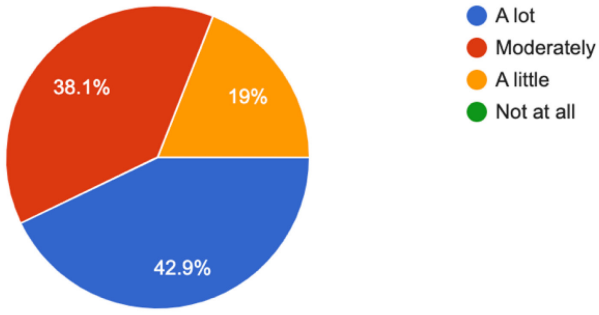
I asked the users if they prefer using biometric technologies over "traditional" security measures, such as keys or IDs access or authentication. The results are as follows:



Preference	Number	Percentage
Yes	15	71.4%
No	5	19%
No preference	1	2.4%
It doesn't matter	1	2.4%
Combination of both	1	2.4%
For things I want quick access to…	1	2.4%

Figure 4: User Preference on Biometric Technology

I asked the users of the survey how much they rely on biometric technologies for everyday life. Out of the 42 responses 16(38.1%) rely on it moderately, 18(42.9%) say they rely on these technologies a lot, and 8(19%) claim they rely on it a little. It was interesting to see that none of the respondents don't rely on biometric technologies at all.

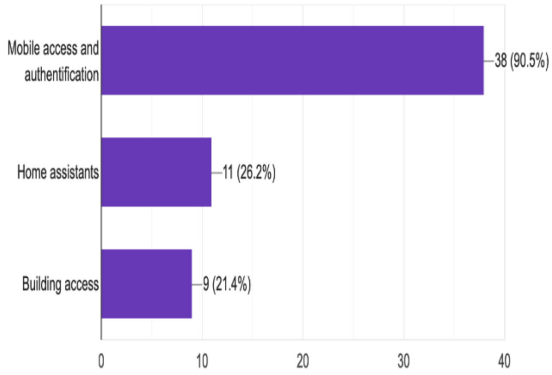


Reliance	Number	Percentage
A lot	18	42.9%
Moderately	16	38.1%
A little	8	19%

Figure 5: User reliance on biometric technologies

Most of my respondents surveyed that they rely on biometric technologies a lot. Considering that most of my respondents are between the ages of 18 and 24, this proves that younger people rely on these technologies to have access to accounts, personal technology, etc.

I asked my respondents in what ways they use biometric technologies to have an idea of the most popular reasons users rely on these technologies.

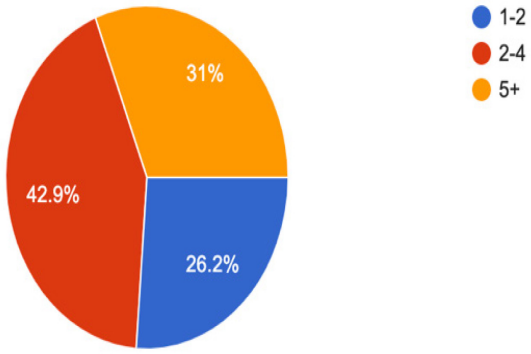


Reasons	Number	Percentage
Mobile access & authentication	38	90.5%
Home assistants	11	26.2%
Building access	9	21.4%

Figure 5: Reasons Users Use Biometric Technologies

The numbers for mobile access and authentication are high for my respondents. Mobile access and authentication use different biometric technologies. It could be facial recognition, fingerprint scanning, voice recognition and more. The least common is using biometric technologies for building access. I'm not surprised to see this low of results for building access because it is common for federal employees to use badges or some other form of identification for building access.

I asked the users of the survey how many passwords they use to safeguard their data. I asked this of them to see if they take the necessary precautions towards protecting precious data. The result is shown below:

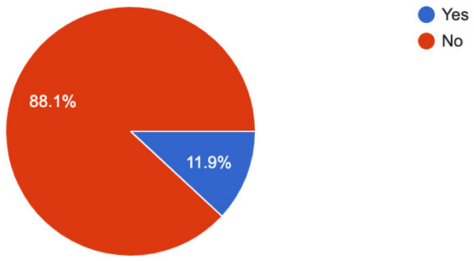


Number of passwords	Number	Percentage
2-4	18	42.9%
5+	13	31%
1-2	11	26.2%

Figure 6: User number of passwords to safeguard data

The results from this show that majority of the user survey respondents only use between 2-4 passwords in total to safeguard all their personal information from cyberattacks. Passwords provide the first line of defense against unauthorized access to your computer and personal information. Considering almost majority of the participants rely on biometric technologies a lot, the results for the number of passwords used to safeguard data is dangerously and concernedly low.

Lastly, I asked the users of the survey if they have ever experienced any form of attack on a biometric database.



All but five said no. I asked for the users to briefly describe their experience of successful or potential biometric hacking. One respondent stated "Employer/agency emails supposedly sent by staff with instructions to click on a link. I'm aware to scam over links/emails if questionable or if not alerted by sender previously." From this, I can conclude they are a government employee. Other descriptions include:

- "Almost got my bank account hacked."
- "Someone knowing my email and sending an email to change my password"
- "Someone was able to hack my credit card and commit fraud"
- "Someone in Russia was logged into my personal email. I had to change my passwords…"

IV. Analysis of Results

A. Biometric Usage

I want to prove that the younger population is more susceptible to risk because of the increased use of biometric technologies compared to the older population. My survey shows that majority of the respondents, 76.2%, are between the ages of 18-24 and majority prefer to use biometric technologies over traditional security measures. The younger population uses these technologies mainly for the purpose of convenience. While the underlying mechanisms for biometric authentication are sophisticated, they are remarkably simple and rapid for users. It's faster to put your finger on a scanner and unlock an account in seconds than it is to type out a long password with several special characters.

From my results, biometrics represent unique threats to young adults, in addition to the data security and privacy problems that apply to other biometric applications. Because this technology was created primarily for adults, it may not perform as well when utilized with youngsters. Errors in biometric recognition can lead to the exclusion of marginalized and disadvantaged populations from vital services and create extra barriers for them.

My results show increased use of biometric by the younger population. This could be a direct result from the ageing process posing a problem for biometrics. Biometrics has long sought universal (everyone has them), collectable (easily measured in everyone), and permanent (they don't change, and no one loses them) methods. However, no biological characteristic perfectly fits all three criteria. No trait is completely permanent: they all decay (or at least vary) as we age, and the ones that are the most permanent (such as DNA) are the most difficult to collect. Thus, there are two major issues. First, because biometric traits diminish with age, the quality of a picture captured from an older person is likely to be worse than that of a younger person, resulting in higher failure to capture or enrollment rates. Second, because biometric traits fluctuate over time, 'internal variation' and 'template ageing' can degrade system performance significantly.

B. User Preference

In section one, I mentioned the moment that biometric data is recorded it is at high risk because it can be easily tampered with or altered in some way. My results show that 90.5% of respondents use biometrics for mobile access and authentication. Using biometrics in these ways are better than traditional measures because it is both convenient and safe. My survey results show that biometric technologies are not used very often for building access (21.4% of respondents use biometrics for this reason). Biometric authentication is difficult to duplicate since it relies on unique traits for verification. Passwords and ID cards, for example, are not as safe because they can be readily stolen or guessed.

Face recognition, like any other technology, has potential downsides, such as risks to privacy, abuses of rights and personal freedoms, data theft, and other crimes. There's also the possibility of mistakes owing to technological problems.

From my results, it is evident that 71.4% of respondents prefer using biometric technologies over traditional security measure like keys and IDs. Is it effective to ask if young adults feel comfortable with biometric security measures *replacing* the traditional password for their day-to-day security? Of the biometric options available, the survey discovered the most support towards mobile access and authentication, with over 90% favoring this method, possibly influenced by the adoption of newer iPhone and Galaxy mobile devices. The survey also found that younger adults, which is the majority of the survey, appear moderately security conscious, with 42.9% of respondents admitting to only having 2-4 variations of

passwords across the many accounts and technologies requiring pins or some form of password authentication.

V. Conclusion

Biometric technology is on the forefront of technology advancements in the world. It is seen in almost every industry, some being the government, enterprise, and banking. With this advancement in the technology field, companies are utilizing this “safe” and “convenient” tool to sell their products to consumers. Although this convenience tool is reached across every inch of the population, the younger group is taking advantage. This makes them more susceptible to risks without them even knowing. Users must be aware that biometric databases can be targeted by hackers, placing the users at danger of identity theft. They might not be able to do anything if this happens. A password may be changed at any time, but fingerprints and eyeballs cannot.

Biometric technology is quickly evolving, and it will undoubtedly play an increasingly important part in modern life. This expansion is driven by the need for increased security in the battle against cybercrime. COVID-19 is also boosting demand for contactless biometrics in applications such as doors, bathroom fixtures, and elevator buttons. Biometrics, in the end, have nearly limitless potential in a variety of fields. They also have the advantage of effortlessly blending into human workflow [8]. Each of these biometric technologies, including fingerprint identification, iris and retina scans, facial recognition, gait, voice, DNA, brain waves, and more, can be used to effectively identify and authenticate humans by combining physiological or behavioral features of any individual human with information from digital databases that describes the individual's identity.

With millennials rapidly becoming the largest generation in the workforce, IBM predicts that these trends will have an impact on how employers and technology businesses provide access to gadgets and apps in the near future. As risks to their digital identity continue to increase, respondents recognized the benefits of biometric technologies such as fingerprint readers, facial scans, and voice recognition. Young adults favor convenience above security. A faster sign-in experience is favored over a more secure type of verification. This could be one of the reasons why millennials are more likely to use biometric authentication than those over 46.

The Future of Biometric Technology

Biometric technologies are increasingly becoming ingrained in people's daily lives all around the world. Many of us use biometric authentication on a regular basis as a result of mobile device integration. Medicine, finance, marketing research, and a variety of other industries that require personal identity will all benefit from biometric trends in the future.

The question of whether biometric technologies will ever be completely secure has yet to be answered. Nonetheless, it will continue to transform how we conduct online transactions. Because of their speed and convenience, these automated solutions will be widely used.

As people continue to disclose their biometric information to many platforms and providers, the risks to security and privacy will grow. The truth is that biometric technologies rely on a centralized database, and any hacker with malevolent intent can exploit a computer network to steal data. We need stronger and more sophisticated security services as hackers lift their game and change tactics.

Increased education and understanding about how biometric data is processed and kept is required to avoid identity theft and safeguard against fraudulent conduct. As more stakeholders see biometric technology's enormous potential, countries throughout the world are pushing to enact rules.

People's rights must be adequately secured, and their data in the hands of both commercial and public entities must be managed wisely and sensibly, according to these standards. These global movements demonstrate that biometric technologies are rapidly evolving, and legislation must follow pace. To safeguard digital data and ensure that biometric technology will properly shape human identity authentication applications, difficult technological, people, process, and policy concerns must be solved.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

[1] Aarp. (2021, April 21). *Tech usage among older adults skyrockets during pandemic*. Tech Usage Among Older Adults Skyrockets During Pandemic. Retrieved November 3, 2021, from https://www.prnewswire.com/news-releases/tech-usage-among-older-adults-skyrockets-during-pandemic-301273924.html.

[2] Beranek, B. (2021, February 8). *Ai and biometrics in 2021: Predictions, trends, and insights for what might lie ahead*. Security Magazine RSS. Retrieved November 3, 2021, from https://www.securitymagazine.com/articles/94548-ai-and-biometrics-in-2021-predictions-trends-and-insights-for-what-might-lie-ahead.

[3] *Biometric aging - effects of aging on Iris recognition*. (n.d.). Retrieved November 3, 2021, from https://www.mitre.org/sites/default/files/publications/13-3472-biometric-aging-iris-recognition.pdf.

[4] *Biometrics and security*. Biometrics and Security | Center for Strategic and International Studies. (n.d.). Retrieved November 3, 2021, from https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-6.

[5] *Cyber security: The future risk of biometric data theft*. – CNA Hardy. (n.d.). Retrieved November 3, 2021, from https://www.cnahardy.com/news-and-insight/insights/english/cyber-securit-the-future-risk-of-biometric-data-theft.

[6] Galbally, J., Haraksim, R., & Beslay, L. (2019, May 5). *A Study of Age and Ageing in Fingerprint Biometrics*. IEEE.org. Retrieved November 3, 2021, from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8509614&tag=1.

[7] Galbally, J., Martinez-Diaz, M., & Fierrez, J. (2013, July 23). *Aging in biometrics: An experimental analysis on on-line signature*. PloS one. Retrieved November 3, 2021, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3720939/.

[8] Kaspersky. (2021, January 13). *What is biometrics security*. www.kaspersky.com. Retrieved November 3, 2021, from https://www.kaspersky.com/resource-center/definitions/biometrics.

[9] Llc, L. (2020, April 28). *Biometrics and cybersecurity* . LIFARS, Your Cyber Resiliency Partner. Retrieved November 3, 2021, from https://lifars.com/2020/05/biometrics-and-cybersecurity/.

[10] McDonald, C. (2015, January 20). *Younger users prefer biometrics to passwords*. ComputerWeekly.com. Retrieved November 3, 2021, from https://www.computerweekly.com/news/2240238497/Younger-users-would-rather-have-biometrics-than-passwords.

[11] Sasse, A. M., & Krol, K. (n.d.). *Usable biometrics for an ageing population - UCL discovery*. Retrieved November 3, 2021, from https://discovery.ucl.ac.uk/id/eprint/1427686/2/Usable_biometrics_for_an_ageing_population_online_VERSION_A.pdf.

[12] *The top 9 common uses of biometrics in everyday life - NEC NZ*. NEC. (2021, October 11). Retrieved November 3, 2021, from https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/.

[13] *Transport and climate change: A review - citeseerx.ist.psu.edu*. (n.d.). Retrieved November 3, 2021, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.7623&rep=rep1&type=pdf.

[14] Vitak, J. (2020, September 25). *Trust, privacy and security, and accessibility considerations when conducting mobile technologies research with older adults*. Mobile Technology for Adaptive Aging: Proceedings of a Workshop. Retrieved November 3, 2021, from https://www.ncbi.nlm.nih.gov/books/NBK563116/.

[15] Zielinski, D. (2021, July 7). *Use of biometric data grows, though not without legal risks*. SHRM. Retrieved November 3, 2021, from https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/biometric-technologies-grow-.aspx.

Appendix

The survey questions used to feedback on biometric usage and risks across the different age groups are below. These are the questions that comprised my survey:

1. Select your age range
2. (Biometric technologies generally refer to the use of technology to identify a person based on some aspect of their biology) What technologies do you use? Choose all that apply.
3. Do you prefer using biometric technologies over "traditional" security measures? ex. Keys, IDs
4. How much do you rely on biometric technologies?
5. In what ways do you use biometric technologies? Choose all that apply.
6. How many passwords do you use to safeguard your personal data?
7. Hackers can target biometric databases, putting people at risk. Have you ever experienced this or any form of it?
8. If yes, briefly describe your experience.