Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2019 Proceedings | Southern (SAIS)

3-22-2019

A Brief Look into Biometrics and One Use in Higher Education

Lillian Lukyamuzi
Georgia College & State University, lillian.lukyamuzi@bobcats.gcsu.edu

Sonny McKenzie
Georgia College & State University, sonny.mckenzie@gcsu.edu

Christopher Parks
Georgia College & State University, christopher.parks@bobcats.gcsu.edu

Tiffany Smith
Georgia College & State University, tiffany.smith2@gcsu.edu

A BRIEF LOOK INTO BIOMETRICS AND ONE USE IN HIGHER EDUCATION

Lillian Lukyamuzi
Georgia College & State University
lillian.lukyamuzi@bobcats.gcsu.edu

Sonny McKenzie
Georgia College & State University
sonny.mckenzie@gcsu.edu

Christopher Parks
Georgia College & State University
christopher.parks@bobcats.gcsu.edu

Tiffany Smith
Georgia College & State University
tiffany.smith2@gcsu.edu

ABSTRACT

Biometrics for the purpose of identification is not a new concept, nor is it limited to one specific field. Both physical and biological unique characteristics are utilized today by biometric technology as a means of recognition (Krishan & Mostafavi, 2018). How exactly are biometrics used today in authorization and identification systems? What are some of the advantages biometric technologies over traditional methods of authentication? What are some of the security and privacy concerns of biometric technology? In this paper, by reviewing multiple published articles in the field of biometrics, we seek to answer these questions, provide insight into the future of biometrics, and discuss the varying responses that biometrics has received from end users, including biometric legislation. We will then look deeper into one particular area of biometric technology, voice recognition, by proposing research in higher education to be conducted on this subject.

Keywords

Biometric(s), authentication, security, privacy, legislation, higher education, voice recognition

INTRODUCTION

As technology expands across varying disciplines, the topic of biometrics is gaining attention, particularly in identification and authentication methods. At the base level, simply recognizing someone's voice is a form of biometric identification (Krishan & Mostafavi, 2018; Mann & Smith, 2017). Yet, during this age of expansion of technology, the use of physical attributes as an identification method has become more sophisticated. Several forms of biometric data are currently used for authentication and identification purposes. For example, cell phones have fingerprint sensors and, more recently, facial recognition as an unlock method as well as a method of making mobile payments (Chatzky, 2018). Whether you are aware of it or not, the use of biometric technology surrounds us each day. Law enforcement, healthcare, mobile phones, higher education, banking, and manufacturing - these seemingly different areas all contain one common factor: biometric technology (Gemalto, 2018; Dey, Joshi, & Mazumdar, 2018)

LITERATURE REVIEW

Physical and Behavioral Biometrics Explained

Biometric information can be split into 2 different categories: physical and behavioral biometrics (Kamis, Ngugi, & Tremaine, 2011). Physiological (or physical) biometrics refers to some part of a person's anatomy that can be analyzed and recorded. Examples of this type of biometrics include facial recognition, fingerprints, and scans of the retina (Krishan & Mostafavi, 2018). Behavioral biometrics, on the other hand, involve the analysis of a person's behavior. Examples include voice recognition, eye movement patterns, and analysis of a subject's walking gait (Alsaadi, 2015).

Physical Biometrics

Physical biometrics depend on the physical characteristics of an individual (Krishan & Mostafavi, 2018). This technology consists of all fingerprint, facial recognition, hand geometric, iris and retinal scan, and DNA identification methods. According to Kamis et al., physical biometrics are more accurate, due to their stability and many years of research and refinement (2011). They explain that biometric technologies are also harder to copy and do not require remembering passwords (2011). However, the greatest strength of this method is also its greatest weakness. These types of biometrics can be invasive, are expensive, and cannot be revoked if the biometric database is compromised, since a human only has but one set of fingerprints (Kamis et al., 2011; Krishan & Mostafavi, 2018).

Behavioral Biometrics

The second type is behavioral biometrics, which depends on the behavioral characteristics of an individual (Krishan & Mostafavi, 2018). This technology includes typing patterns and keystroke dynamics, voice print recognition, gestures, and more (Gemalto, 2018; Kamis et al., 2011). As opposed to physical biometrics, Kamis et al. note that one of the greatest strengths of behavioral biometrics is that it is non-intrusive to the user (2011). Unfortunately, this technology is not as accurate as physical biometrics. Despite its downfalls, researchers are increasingly looking to behavioral biometrics as an alternative because of their acceptability and low cost (Kamis et al., 2011).

Future Outlook and Development of Biometric Technology

As biometric consumer technology becomes integrated into more devices and services, people are more accepting of it for daily use (Consumer Technology Association, 2016). According to the Consumer Technology Association's report, nearly two-thirds of all consumers support biometric technologies for altruistic purposes and assistive technology (2016). The report also shows that this shift in support demonstrates an understanding of the benefits of biometric technology, creating an enormous amount of opportunity in the biometric industry (2016). Current advancements in various forms of biometric authentication have made the technology more reliable and less intrusive (Friedman, Nixon, & Komogortsev, 2017). Special cameras and sensors embedded into cell phones make facial recognition authentication seamless (Friedman et al., 2017). Also, Friedman et al. states that users expect other social media platforms, in addition to Facebook, to automatically detect faces in pictures that are shared with friends.

Along with incremental advancements in existing methods, there are also emerging biometric identification methods that are currently being explored. Martinovic, Rasmussen, Roeschlin, & Tsudik propose one such method: pulse-response biometrics, which involves analyzing the body's response to a low voltage electric pulse (2017). Each user's skin conductivity will have a different response, allowing this method to uniquely identify individuals (Martinovic et al, 2017). They elaborate by explaining that this method can be integrated into a number pad, allowing it to be analyzed in conjunction with a user entering a PIN (2017). Ear recognition is a relatively new area that is currently being explored. Since the structure of the ear changes very little as we grow, this method could prove to be more suitable as a long-term authentication method (Friedman et al., 2017). As an increased security method, multiple biometric markers can be analyzed simultaneously in a method referred to as multimodal biometrics (Gofman & Mitra, 2016). For example, a user may use a voice print in conjunction with facial recognition when unlocking a mobile device (Gofman & Mitra, 2016).

Authentication vs. Identification

Authentication and identification are two related, but different use cases for biometrics.

Biometric authentication is the process of matching data of the person's characteristics to that person's biometric template for the purposes of identity confirmation or verification (Martinovic et al., 2017). The data stored is compared to the person's biometric data to be authenticated (Gemalto 2018). Authentication is a scenario in which a subject makes a claim to be a specific individual. Ultimately, it answers the question, "Are you who you say you are?" When it comes to authentication, a person is usually trying to unlock something, a phone for example. When you register your fingerprint on a phone, the data is stored, so that when you try to unlock your phone the next time using your fingerprint, the fingerprint you are using now is matched against the fingerprint that was initially stored in the phone.

Identification, on the other hand, does not have the advantage of simply matching against a previously known value, but consists of determining the identity of the individual (Gemalto 2018). Biometric data must, therefore, be matched against a very large data set to determine if there is a match (Martinovic et al., 2017). The goal is to capture an item of biometric data from the individual, which will then be compared to the biometric data of

several other people kept in the database (Gemalto 2018). For example, in identifying a thumbprint, one person's thumbprint would be matched against all thumbprints on file. It answers the question, "Who are you?"

Breach Tactics, Security, and Prevention

A common breach tactic is recovering a biometric characteristic, such as a fingerprint, and then recreating that sample (Adamek, Matýsek, & Neumann, 2015). An attack can also be made on the biometric identification system by disrupting the searching, transmission, or comparing of characters (Adamek et al., 2015). Two common threats are a user's authentication attempts being traced across different applications, as well as a user's distinguishability being compromised (Mitrokotsa & Pagnin, 2017). For example, a user may be traced through using the same authentication across social media applications, like Facebook, Instagram, and Twitter.

Proper security measures, such as encrypting sensitive data and considering the location of storage and matching data beforehand, can be used to help manage cybersecurity attacks (Krishan & Mostafavi 20). For prevention of a breach, a two or three factor authentication combination is recommended, in which the behavioral biometric layer is combined with the current authentication system made of knowledge and token layers (Kamis et al., 2011; Krishan & Mostafavi, 2018). The three factors of authentication are made up of something you possess (such as a card or key), something that you know (such as a password), and something that you are – meaning a biometric sample, such as a fingerprint (Gemalto, 2018). An important prevention measure is for organizations to develop privacy-preserving biometric authentication systems (BAS) – systems that can mitigate certain privacy and security risks, such as stolen biometric data (Pagnin & Mitrokotsa 2017).

Biometric Legislation

To help address biometric security and privacy concerns, biometric legislation is being developed in various states and organizations. Illinois, Texas, and Washington were the first states to implement biometric legislation (Hedges, 2018). As biometric technology continues to grow and develop, it is likely that we will see a growth in privacy and security concerns, as well as policies and procedures to resolve those concerns. It is wise for corporate legal departments to remain vigilant over company use of biometric data, as well as the future legislation of biometric privacy laws (Krishan & Mostafavi, 23).

State of Illinois

The first state law enacted in regards to biometric privacy is BIPA - the Illinois Biometric Information Privacy Act (Krishan & Mostafavi, 2018). BIPA requires informed consent prior to the collection of data, permits only a limited right to disclose, mandates protection obligations and retention guidelines, prohibits profiting from biometric data, and creates a private right of action for individuals harmed by BIPA (Krishan & Mostafavi, 2018).

State of Texas

A year after BIPA was passed, Texas passed the second state law in regard to biometric privacy. CUBI (Capture of Use of Biometric Identifier Act) provides that "a person may not capture a biometric identifier of an individual for a commercial purpose unless the person informs the individual before capturing the biometric identifier and receives the individual's consent to capture the biometric identifier" (Hedges, 2018, p. 47).

State of Washington

Washington State's HB 1493 legislation broadens situations in which disclosure will be permitted, but prohibits enrollment "without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose" (Hedges, 2018, p. 46-47; Krishan & Mostafavi, 2018).

Healthcare Industry

Perhaps the biggest data security and privacy concerns are in the healthcare industry. These concerns are being expressed in the European Union's GDPR (General Data Protection Regulation), one law that is further restricting unauthorized use of personal information (Hedges, 2018). The GDPR specifically recognizes biometric data as a category of sensitive personal data. However, processing of biometric data can be justified under GDPR in certain situations (Krishan & Mostafavi, 2018).

User Response to Biometrics

Since biometric technology necessitates *humans* to interact with a device, effective implementation requires consideration of the perceptions and responses of end users. There is a need to provide convenient and efficient authentication (Thakkar, 2016). With a positive response from many users and successful adoption of various biometric technologies across multiple fields, it is likely that biometrics will continue to grow and have good prospects for the future (Thakkar, 2017). The figure below shows how market intelligence companies expect biometrics technology to grow exponentially over the years, as well as the trends of previous years (Thakkar, 2017).

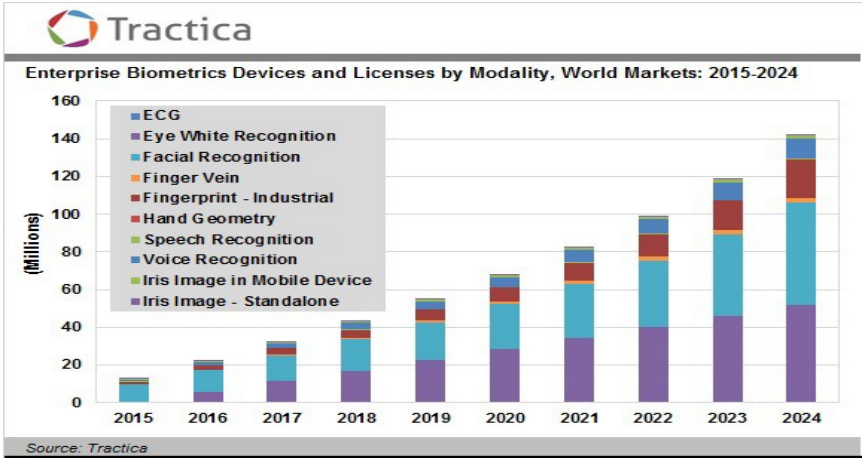

Figure 1. Future Trends (Thakkar, 2017)

Previously, biometrics has been associated to forensics and law enforcement, which made many people skeptical, as capturing fingerprints and other biometric patterns was limited to criminals and anti-social elements (Thakkar, 2016). Currently, with the wide span of the internet, people are more aware of biometrics and realize that being anonymous is impossible in today's digital life (Thakkar, 2016). According to a survey by Visa, 86% of the population is interested in using biometrics to verify their identities to make payments, and Chatzky states that in general, people do not like to use passwords because they are cumbersome and easy to forget, yet biometrics simplifies the process (2018).

Consumers are most familiar with biometrics such as DNA analysis and the biometrics they have seen in the market like fingerprint readers on smartphones (Consumer Technology Association, 2016). Furthermore, according to the Consumer Technology Association's report, most of the adults in the U.S are comfortable using biometrics in areas with high security screening, like the airport and national borders, and almost half of the consumers are comfortable using biometric technologies at home and or the workplace (2016).

As biometrics continues to be used for identification and authentication purposes, people have expressed mixed feelings about it (Thakkur, 2016). Thakkur describes a positive impact of biometrics in that it provides speed and efficiency, as well as job growth in this market (2016). In contrast, he also explains that there are negative social impacts, specifically, many people have expressed concerns about feeling as though the government is continuously tracking their actions and watching over them (2016). It is likely that mixed feelings by society will continue, even as the field of biometrics progresses.

PROPOSED RESEARCH

In our literature review we briefly discussed current and future forms of biometric technologies. One of those biometric technologies is voice recognition. Voice recognition is being used in multiple fields, one of those being higher education. We predict that it will be possible for voice recognition to be used in higher education, and that we will soon see voice recognition technologies used in colleges and universities in the State of Georgia, as well as in higher education across the nation. We spoke with Robert Orr, CIO (Chief Information Officer) at Georgia College & State University who believes voice recognition technology is cutting edge in the higher education industry right now, and that there is a demand for this type of research. In our proposed research study we will explore the possibilities of how voice recognition can be used in higher education, what, if any, colleges and universities are

already using and/or studying voice recognition to be used in higher education, and any obstacles that stand in the way of voice recognition being used in higher education.

Participants and Design

To find our participants in this study, we will start with a university in Georgia and conduct a case study on their experimentation with voice recognition technology. From there, we would contact colleges and universities in the University System of Georgia to see if any of them are conducting research or using voice recognition technologies in their schools. In doing this, we will find out if they have any connections with other colleges and universities throughout the nation who might be conducting research on this topic as well. Finally, we will conduct a thorough search ourselves of universities and colleges across the nation to find out what progress is being made on using biometric technologies in higher education.

With this being such a new and developing topic, we will not set a limit on how many schools that may participate in our research. However, there will be varying levels of participation. At one university we would actually be able to observe some of the experimentation that is being done with the voice recognition software, and would be able to do a thorough case study of their work. For the schools in the University System of Georgia, we might be able to do some in person interviews and possibly some observations as well, depending on which schools are doing work with voice recognition technology. For the colleges and universities throughout the nation, we would rely on phone interviews, surveys and questionnaires to gather information.

Procedure and Measurements

After we confirm which colleges and universities will agree to participate in our study, we would begin by sending out a brief e-mail survey for them to complete. Questions on this survey will include: “Is your institution currently using voice recognition technology?”, “In what ways is your institution using voice recognition technology?”, “Are there any additional ways you see voice recognition technology being used at your institution? If yes, how?” Once we receive the surveys back, depending on their answers, we will reach out to some of the schools for a phone interview, in which a more-detailed questionnaire would be completed. The questions will vary depending on the survey responses, but some questions and requests might include: “Please elaborate more on the type of studies and experimentation your institution is conducting on voice recognition technology.”, “What type of software or other application platforms will you include in your institution’s work with voice recognition technology?”, “What sort of advantages do you see for the use of voice recognition technology at your institution? What kind of obstacles do you see standing in the way of the use of voice recognition technology at your institution?” In both the surveys and interviews we might also include questions about their opinions of voice recognition related to higher education as a whole, not just at their specific institution. Finally, for applicable schools within the University System of Georgia we will contact them to observe their experiments that are taking place with voice recognition software.

As we collect the data, we will store responses in an Excel spreadsheet. We will keep these files on an external hard drive, and we will also encrypt the Excel spreadsheet where it can only be accessed by a password. When all responses have been collected, we will then note any patterns that occur, as well as anything that sticks out as out of the ordinary. We will track consistency of results and any significant progress that has been made. We will also note failures in addition to the successes to see whether or not our predictions are likely or unlikely, based on the consistency of the results we have received. We will then compare our institution with this information to see where we fall on the spectrum of progress being made with voice recognition technology in higher education. Additional follow-up with some of the universities may be conducted if this research is something our own Information Technology department is further interested in.

Conclusion and Discussion

The use of biometric data has made its way into our daily lives. What was once seen as a forensics tool used by law enforcement is now used by individuals to access their personal devices on a regular basis. As this technology continues to improve and grow, users will continue to accept it as commonplace, and we will begin to see biometrics used in even more fields in different ways.

As a research proposal, the results of this study are unknown at this time. It is our plan to talk to enough colleges and universities in the state of Georgia, as well as throughout the country, that we are able to collect and analyze enough data to either support or reject our predictions. A limitation in the study might be that there is simply not enough research being conducted to make a thorough prediction of if it’s possible for voice recognition technology to be

used in higher education at this time, or of its use in higher education. Another limitation to take into consideration is how might private policies, such as FERPA (Family Educational Rights and Privacy Act), be violated? The accuracy of the voice recognition in authentication could also be an obstacle. However, if there are enough schools in higher education conducting thorough research on voice recognition technologies with enough consistent results, the accuracy of those results would be a strength of this proposed study. Another strength will be getting to witness some of the experimentation of this topic firsthand. Ultimately, voice recognition technology is gaining attention in the field of biometrics across multiple industries and is here to stay.

REFERENCES

1. Adámek, M., Matýsek, M., & Neumann, P. (2015) Security of Biometric Systems. *Procedia Engineering, 100*, 169–176. https://doi.org/10.1016/j.proeng.2015.01.355.
2. Alsaadi, I. M. (2015) Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review, 4, 12, 5.
3. Chatzky, J. (2018) *Biometrics are here: The crazy ways you're going to be paying in the future.* Retrieved from https://www.nbcnews.com/better/business/biometrics-are-here-crazy-ways-you-re-going-be-paying-ncna872336.
4. Consumer Technology Association. (2016) *Biometric Technology Enjoys Strong Support from Consumers, Says CTA.* Retrieved from https://www.cta.tech/News/PressReleases/2016/March/Biometric-Technology-Enjoys-Strong-Support-from-Co.aspx.
5. Dey, S., Joshi, M., & Mazumdar, B. (2018) Security Vulnerabilities Against Fingerprint Biometric System. *Indian Institute of Technology, 2018*.
6. Friedman, L., Komogortsev, O. V., & Nixon, M. S. (2017) Method to assess the temporal persistence of potential biometric features: Application to oculomotor, gait, face and brain structure databases. PLOS ONE, 12, 6. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0178501.
7. Gemalto. (2018) Retrieved from https://www.gemalto.com/govt/inspired/biometrics.
8. Gofman, M. I., & Mitra, S. (2016) Multimodal biometrics for enhanced mobile device security. *Communications of the ACM*, 59,4, 58–65.
9. Hedges, R. (2018) Privacy and Security Risks with Biometrics. *Journal of AHIMA.*
10. Kamis, A., Ngugi, B., & Tremaine, M. (2011) Intention to Use Biometric Systems. *Intention to Use Biometric Systems*, 20-46.
11. Krishan, R., & Mostafavi, R. (2018). Biometric Technology: Security and Privacy Concerns. *Journal of Internet Law*, 22,1, 19. Retrieved from https://gcsu.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=131103595&site=eds-live&scope=site.
12. Mann, M. & Smith, M. (2017) Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *University of New South Wales Law Journal, 2017*.
13. Martinovic, I., Rasmussen, K., Roeschlin, M., & Tsudik, G. (2017). Authentication Using Pulse-Response Biometrics. *Communications of the ACM, 2017*.
14. Mitrokotsa, A. & Pagnin, E. (2017) Privacy-Preserving Biometric Authentication: Challenges and Directions. *Security and Communication Networks, 2017*. Retrieved from https://www.hindawi.com/journals/scn/2017/7129505/
15. Thakkur, D. (2017) *Biometrics: Cost, Types, and Comparative Analysis, 2017.* Retrieved from https://www.bayometric.com/biometric-devices-cost/
16. Thakkur, D. (2016) *How does Biometric Technology impact Society?* Retrieved from https://www.bayometric.com/biometric-technology-impacts-society/