On the Expected Increase in Mobile Transactions Authenticated Through Biometrics

Loren Barcenas & Koray Karabina

Biometrics, the identification of specific individuals by unique physical characteristics – like fingerprints, irises, or facial features – promises greater convenience and security than traditional methods since physical features cannot be lost or forgotten. Our study explores practical implementations of biometrics, especially its projected growth in the field of mobile transactions. Our study supports the claim that usage of biometric systems, especially in the authentication of mobile transactions, will significantly increase despite security and privacy breaches. Because biometrics is a relatively new technology with little previous data, we circumvent this issue by correlating its usage to that of smart phones to analyze statistics to create regression analyses. According to our findings, the number of biometric users will increase from $7.72 billion in 2014 to $10.26 billion in 2019, thus it would be prudent to invest in biometrics by implementing more systems, and creating more reliable systems based on new standards.

• • •

INTRODUCTION

Our study supports the notion that users of biometric identification will rise over time. Biometric identification is the verification of a specific individual's identity based on a unique physical characteristic that all people typically possess; such as fingerprints, faces, or irises (Maltoni, Maio, Jain, & Prabhakar, 2009). This method directly identifies the user, rather than traditional methods that identify something the user knows or owns, such as passwords or swipe cards (Maltoni, Maio, Jain, & Prabhakar, 2009). These can be shared, stolen, or lost, unlike biometric identifiers, making the latter option potentially more secure. Biometric identification was originally implemented in criminal cases by law enforcement, however its potential to decrease identify fraud makes it more widely applicable (Maltoni, Maio, Jain, & Prabhakar, 2009). Other instances in which it is already used today include entrance at theme parks, smart phone devices, border control, and mobile banking. The reach of biometrics is sure to expand to many other applications in the future, as it is a useful and flexible technology.

These systems function by first requiring an enrollment phase in which the biometric trait is presented and a software algorithm extracts salient characteristics to create a biometric template associated with the individual, which is stored in the database (Jain & Nandakumar, 2012). Then, when the enrolled user needs to be authenticated, he or she presents the same biometric trait, called a query, which is compared to the template by a biometric matcher that produces a matching score reflecting the similarities of the samples (Jain & Nandakumar, 2012). If the matching score passes a predetermined threshold it is accepted, and if not, it is rejected.

This type of identification poses certain inherent limitations since matches will not be completely perfect due to minor changes in the biometric trait, such as a scar on a finger, facial accessories, or even presenting the trait at a different angle or rotation. This produces two types of errors called false negatives and false positives. False negatives occur when an enrolled user is denied access due

to low match similarity, which could be caused by poor sensor quality or changed positioning of the biometrics trait (Jain & Nandakumar, 2012). False positives occur when two different biometric samples are deemed similar enough to be matches and an un-enrolled attacker gains access (Jain & Nandakumar, 2012). Additionally, there are adversarial attacks, deliberate attempts to manipulate the system to gain access without enrolling (Jain & Nandakumar, 2012). Such attempts include what are known as spoof attacks, in which one presents a non-living fake biometric trait to the sensor (Jain & Nandakumar, 2012). One way to prevent spoof attacks would be to include liveliness tests to ensure the biometric sample being collected is in fact from a live user. Other more cryptographic attacks include what are called hill-climbing attacks and template reversing attacks. During a hill-climbing attack, the biometric feature is artificially tweaked to increase the matching score until the threshold of acceptance is reached (Martinez-Diaz, Fierrez-Aguilar, Alfonso-Fernandez, & Ortega-Garcia, 2006). A template reversing attack constitutes a hacker retrieving the biometric template, which is stored after enrollment, and using reverse engineering along with computational tools to revert it into the original biometric trait (Boulgouris, Plataniotis, & Micheli-Tzanakou, 2009). Cryptographic methods are deployed to protect against these attempts at fraudulent verification. Although there may be certain limitations to biometric technology, it is still believed to be more efficient and accurate at identification than traditional methods on average.

The purpose of our study is to explore whether the claim that usage of biometric systems will increase over the years. This will be done by analyzing current statistics and past trends to create regression analyses, as well as tables based on logical reasoning that follow from plausible assumptions. Such evidence would provide companies with the necessary data to confidently invest in biometric features, as well as motivate policy makers to regulate its usage.

EXISTING APPLICATIONS

Though it is a new technology, biometric systems are already being put to use in everyday life. Due to the versatile nature of biometric technology and the need for identification, biometrics can be used in different settings including the government, the healthcare and finance industries, as well as through mobile devices. This section will detail current methods in which biometrics are employed to provide a sense of their usefulness.

Government

One of the biggest instances in which biometric systems are deployed today is at customs and border control. In the United States, specifically, this technology is still in its beta phase. The Apex Air Entry and Exit Re-Engineering Project, created by Customs and Border Control (CBP) under the authority of the Department of Homeland Security, consists of three pilot programs (Bicchierai, 2015). The first of which, called The 1:1 Facial Recognition Entry Pilot program, has customs officers take a picture of randomly selected Americans, regardless of their consent, and uses a facial recognition algorithm developed by the CBP to compare it to their passport photo (Bicchierai, 2015). This serves to increase the country's security by providing a more effective way to identify individuals who may pose a threat to homeland security. The second initiative of CBP is the Biometric Exit Mobile Experiment, during which foreigners exiting the US will be regulated by CBP officers most likely using finger scanners that identify the individual and compare their information to that which they provided upon entrance to ensure that the non-citizens have not overstayed their permitted time (Biccierai, 2015). Finally, the third pilot program, Pedestrian Biometric Experiment, replaces entry kiosks at the Otay Mesa border between the US and Mexico with devices that scan the faces and irises of travelers, in effect, increasing security measures and reducing public safety threats.

Another place in which biometrics is taking off is India. The Unique Identification Authority of India (UIAI) has associated each citizen with their respective demographic information, such as name, date of birth, address, and gender, with their biometric traits including a photograph, each fingerprint, and iris scans of each eye (Gerdeman, 2012). Indian citizens have benefitted from being identified and documented since many residents did not have any official ID needed to obtain most government services, such as ration cards or bank accounts (Gerdeman, 2012). Moreover, the UIAI reduces the incidences of fake IDs being used to fraudulently receive government benefits.

Health Care Industry

In the health care industry, clinicians can use biometric systems to pull up and manage patient records. One company, Imprivata, provides software that allows clinicians to scan their fingerprint at any workstation in order to verify their authorization to view medical records instead of having to log in numerous times throughout the day (Imprivata, Inc., 2014). Expediting the process in this way not only leaves more time for patient care, but also complies with HIPAA password policy regulations and heightens security (Imprivata, Inc., 2014). Another program Imprivata offers is called PatientSecure which links patients to their medical records via palm vein recognition (Imprivata, Inc., 2014). This allows enrolled patients to be quickly identified when they scan their palm in order to retrieve their medical files. The user friendly and non-intrusive qualities of palm vein recognition cause it to have a high acceptance rate among users (Imprivata, Inc., 2014).

Finance Industry

In the finance sector, a new technology has become available that combines biometrics with credit cards. MasterCard has teamed up with Zwipe to create a credit card that eliminates the need for a PIN number (Chowdhry, 2015). Instead, after initially enrolling your fingerprint, you hold the card with your finger against the scanner on the card while waving it over a near field communication (NFC) compatible terminal (Chowdhry, 2014). Not only does it increase efficiency and usability, it is even more secure since the fingerprints are stored on the individual cards rather than an external database (Chowdhry, 2014). Payment through biometric identification is very convenient commercially in that consumers are always looking for more efficient, yet secure, ways to make purchases. Meanwhile vendors also benefit since buyers are more likely to impulse shop due to the expedited nature of using biometric identification systems.

Mobile

Biometrics can also be used to make payments through mobile devices. The two largest players are Apple and Samsung. Both big name companies have fingerprint authentication digital wallets, Apple Pay and Samsung Pay, which have recently been implemented. The digital wallets function by storing credit and debit card information, which is verified as the owner's by a biometric trait (fingerprint for Apple, or retina, iris, voice, face or fingerprint for Samsung), which allows the surface of the screen to be waved over a NFC scanner to complete a transaction (Seals, 2014). Eliminating physical cards like this benefits customers by reducing the instances in which hackers may lift card data from point-of-sale machines (Seals, 2014).

SECURITY AND PRIVACY ISSUES

Although there are countless practical applications of biometric systems, risks also exist. One such risk includes security breaches, which can be defined as an unauthorized person gaining access to sensitive or confidential data.

In addition to security issues, another type of risk is a privacy breach. A breach in privacy occurs when personal information becomes available to unauthorized individuals that can potentially harm the individual about whom the information described. Although privacy and security may seem similar, they are in fact distinct categories. Using credit cards to illustrate the difference, if someone's credit card number was stolen, it would be a breach in security as the thief does not have any information about the specific individual, besides perhaps their name, but may still inflict harm on them financially by using the credit card fraudulently. On the other hand, if a hacker was able to learn your shopping habits, for example that you shop at Macy's on every one day sale, or that you bought a pregnancy test, it could reveal a piece of personal information that you may not wish to disclose.

Although using biometrics for authentication is harder to fake or steal, it is still possible, and the resulting effects are greater. Since biometric information cannot be changed or re-issued, if it were to be stolen, protecting security and privacy becomes more difficult, and consequently more problematic, as there is far more personal information associated with biometric data than a randomly generated credit card number or a bank account (Sadowski, 2015).

Government

Although governments have begun to employ biometric systems to solve security issues in border control and for identification purposes, biometrics is still in an early phase and has been compromised.

The United States Office of Personal Management (OPM) issued a statement in June 2015 announcing that its security had been breached by a Chinese cyber-attack and the fingerprints of at least 5.6 million individuals had been stolen, thus constituting a privacy breach as well (Otto, 2015). Information breaches like this are worrisome and should be protected against at all costs because it gives adversaries the ability to create a database of personal information about citizens that could be used to identify intelligence agents or defense personnel, which is exactly what experts predict China is doing (Sanger, 2015). Although the ability to abuse fingerprint data is currently limited, it will grow in the future as biometric systems are being increasingly implemented by government facilities, private companies, and personal devices.

Industry Specific

As previously mentioned, the health care industry, insurers, and clinicians alike can benefit from the usage of biometrics for secure identification. However, it can be risky during the infancy of this technology since there are still bugs to be worked out, and a breach in a healthcare system's security could cause major privacy issues. The systems of Anthem, a US health insurance company, were compromised in late January of 2015, exposing the names, dates of birth, home and email addresses, medical IDs, and social security numbers of up to 80 million customers and employees (Osborne, 2015). Although no medical or financial information is believed to have been stolen, it raises concerns that health care companies will be targeted for private data highly valued on the black market (Harwell & Nakashima, 2015). Medical records are now worth $10 on the black market, which is ten to twenty times the value of credit cards at $0.50 - $1 (Humer & Finkle, 2014). This can be attributed to the ability to freeze and cancel credit accounts after immediately detecting fraud, however, medical identity theft can go undetected by both patient and provider for years. Medical information in the wrong hands could lead to fraudulently filed insurance claims or stolen prescription drugs, which is estimated to amount to tens of billions of dollars in loss annually (National Health Care Anti-Fraud Association, 2015). These possibilities coupled with the fact that health insurers, in general, do not have as high security as most financial companies makes health care one of the most highly sought targets for hackers (Harwell & Nakashima, 2015). Thus, it would be beneficial to implement biometric systems in order to safeguard private medical data more securely.

Mobile

While Apple Pay and Samsung Pay have been widely received positively, there may be setbacks with the integration of fingerprint technology in mobile devices. Within less than a week of the release of the iPhone 5s, hackers were able to gain access to the devices fraudulently despite expert opinions that fingerprints could not be foraged that easily (Revilla, 2015). This was achieved through a hack method called a gummy finger attack, essentially extracting a fingerprint artificially and presenting the non-living sample to the scanner (Jain & Nandakumar, 2012). Therefore, a hacker could either lift someone's fingerprint off of something they touched or take a high definition photo of their fingers to create a rubber copy with a 3D printing machine to which the phone will grant access (Seals, 2014). There are also more sophisticated ways of obtaining fingerprint images or bypassing security altogether. Di Shen, a security researcher, presented at the Black Hat Conference 2015 on his findings about how to exploit the Trusted Execution Environment, the section of a device that is supposed to be isolated and completely secure, of a Samsung phone (Shen, 2015). His findings stated, "a local application is able to get fingerprint images or other encrypted data, disable signature verification of modem image and TA, load any module to TEE and modify the efuse data," (Shen, 2015) thus illustrating the imperfect condition of current security in mobile devices.

RISK TO BENEFIT TRADE-OFF

It is widely known that if an application has many benefits, it will attract a large base. Additionally, one might be inclined to believe that if another such application had many privacy or security risks, the general population might be hesitant about using it. This leads to what we call the risk–benefit tradeoff; the idea that an application's benefits outweigh the potential risks or vice versa. The perceived risk–benefit tradeoff is important to note when analyzing willingness to use a new technology since it is well known that most social media sites do not have strong privacy policies, but

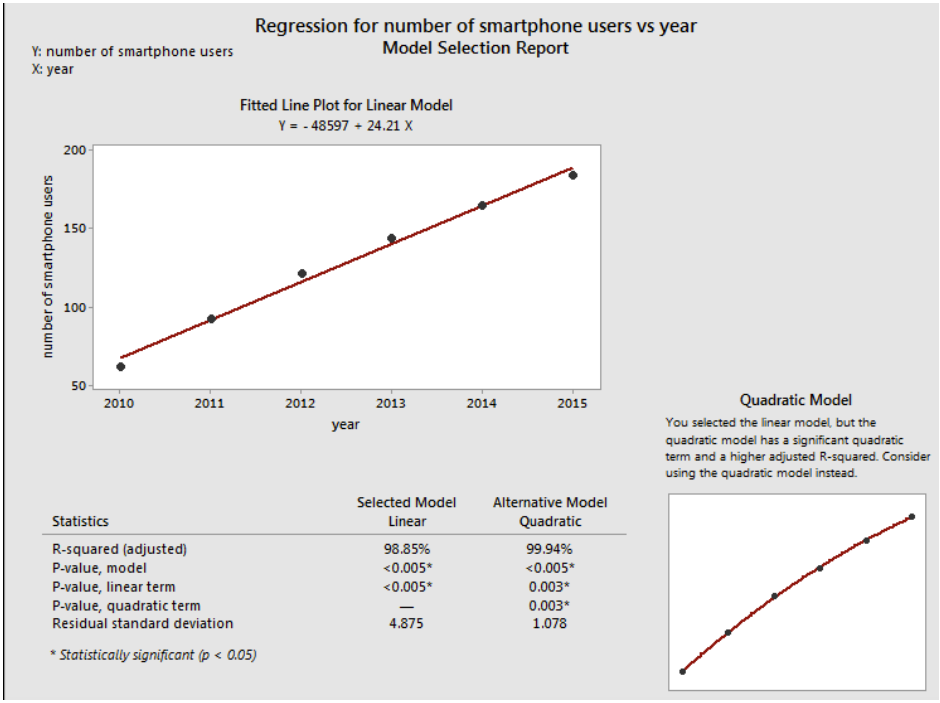

FIGURE 1: **This regression analysis was created using data regarding the number of smartphone users over the years from a statistics company called Statista in software called Minitab.** A linear model was used rather than a quadratic model, as there was a discrepancy with the quadratic model in that after reaching the apex, the values would decrease toward negative infinity, which is not logical in this situation. A logarithmic model would perhaps be most realistic, however the available software did not support that option.

are popular nonetheless, presumably due to their high-perceived benefits.

For example, Facebook revealed in June 2013 that it had accidentally leaked six million users' private information, such as email addresses and phone numbers to third parties over the course of a year. After publically admitting the mishap, Facebook stated that they had not received any customer complaints (Shih, 2013). Moreover, according to Statista , the number of Facebook users in the United States from the year 2013, when the privacy leak was revealed, to the next year did not drop, but in fact increased by 4.9 million (Statista, 2015), 2015) This goes to show that the public may be willing to overlook breaches in security or privacy if a service is seen as beneficial enough.. This goes to show that the public may be willing to overlook breaches in security or privacy if a service is seen as beneficial enough.

REGRESSION ANALYSIS

The purpose of this section is to analyze the trend in number of biometric transactions to determine if it is growing, especially via mobile mediums.

Hypothesis: As we have previously noted, there are risks of privacy leaks and security breaches, however, this will not have a significant negative effect on the usage of biometric systems because user perceived benefits will outweigh perceived risks.

Support: First, as companies use white hat hackers to identify the bugs in their systems, new updates will be released that are even more secure

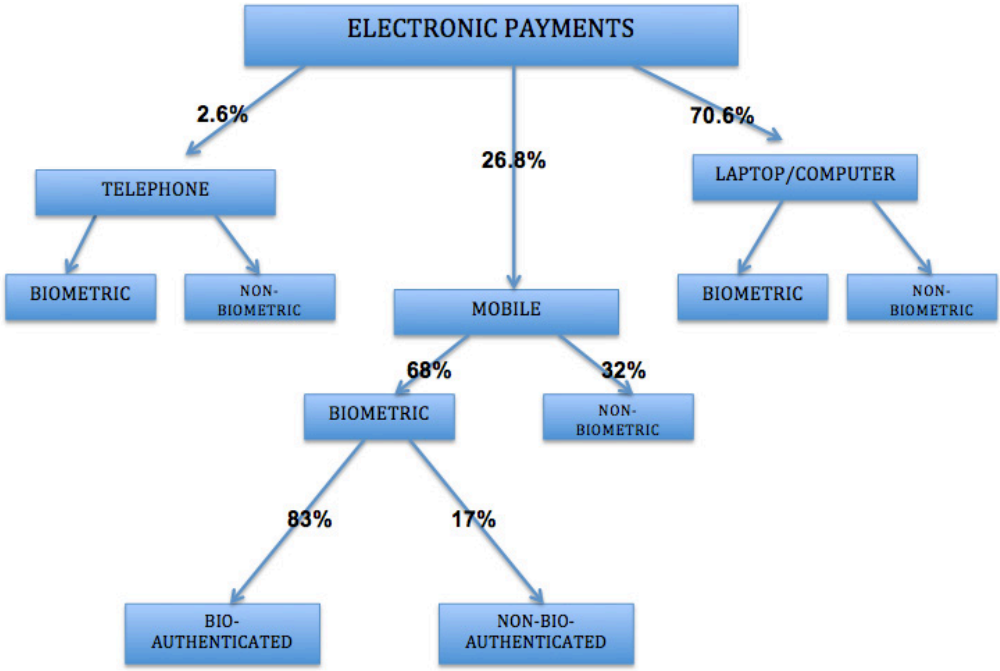

FIGURE 2: **This flow chart illustrates a breakdown of the percentages of the different ways electronic payments were made in 2014 and are assumed to stay constant.** The percentages that are not shown under telephone were left out since they are so small they would be negligible. The percentages under laptop/computer were left out since there is not much information regarding biometric usages through those mediums due to the fact that biometrics is not largely used on laptops or computers, so they can be regarded as negligible as well.

than previous versions. This is evidenced by the existence of hacker conferences such as the "Black Hat Conference" wherein many devices are reviewed and thereafter improved (Shen, 2015). The security teams of specific companies also work to update their systems, as demonstrated when Facebook's team stopped the leak within twenty-four hours of being notified about it (Shih, 2013).

Additionally, as time progresses and biometric systems are used more commonly on larger scales, solid standards will be established to ensure that each unit's security system is high quality. One such standard establishing organization is the FIDO (Fast IDentifying Online) Alliance whose mission it is to "change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services" (FIDO Alliance , 2015). Once a set of common standards is established making systems more reliable and easy to operate, users will feel more secure, thus causing the population of biometric users, and therefore transactions authenticated by biometrics, to grow.

Hypothesis: Since biometric systems are a fairly new technology, we do not have sufficient data to create a regression line to predict future usage. To navigate around this issue, we claim that biometric system usage resembles that of smart phones.

Support: The assumption that these two data directly correlate to one another is based on the fact

	Percentage of mobile payments authenticated via biometrics	Quantity of money made through mobile payments	Money made through mobile payments authenticated through biometrics
2014	0.68*0.83*26.8 = 15.13%	$51 billion	$7.72 billion

TABLE 1: **This table serves to illustrate how the percentage of mobile payments authenticated via biometrics was calculated, as well as how we arrived at the quantity of money made through mobile payments authenticated through biometrics.** The percentages from the previous figure leading to bio-authenticated biometric mobile devices were multiplied together to find the total percentage of mobile payments authenticated via biometrics, 15.13%. The quantity of money made through mobile payments in 2014 was found on the site Statista. Then 15.13% was multiplied by $51 billion, the quantity of money made through mobile payments, to obtain $7.72 billion, the money made through mobile payments through biometrics.

that more smart phone companies are incorporating biometrics by using fingerprint scanners to unlock phones. It is also assumed that those who are interested in using new technology, such as smart phones, will also be willing to use biometrics in other applications. This is based on the notion, supported by scientific study, that acceptance of technology in general is based on user trust and interest in it (Miltgen, Popovic, & Oliveria, 2013). Thus, if we analyze the upward trend in the number of smartphone users, as reported by Statista , we can use it to draw conclusions about the trend in the number of users of biometric systems. Figure 1 is a linear graph depicting the rate (24.21) at which smartphone users will increase over time. As explained above, it is comparable to the rate at which biometric users will increase over time and will be used in the prediction of future transactions authenticated through mobile biometrics.

Hypothesis: We predict that biometrically authenticated mobile payments will dominate e-commerce in the US beginning at $7.72 billion spent in 2014, increasing to $10.26 billion in 2019.

Support: In 2014 alone, about 26.8% of e-commerce payments were made through mobile phones and tablets (Statista, 2014). Samsung and Apple products made up about 68% of those products (Cheng, 2014). We can assume that every iPhone and Samsung smartphone will have a biometric sensor by the year 2016, as they are already being incorporated and are unlikely to be removed in newer models. Other cell phone and tablet companies are likely to follow with their own versions of biometric sensors as well, making our percentage of biometric capable devices on the lower end. Additionally, according to USA Today, 83% of iPhone 5s users reported using the Touch ID biometric feature to unlock their phones (Stephans, 2014). Thus, we can assume that about roughly the same percentage of people will be likely to authenticate a transaction using biometric techniques since they felt comfortable using it to unlock their phone. These statistics are visually represented in the breakdown of how electronic transactions are paid in Figure 2.

Based on the above statistics, we can calculate that the percentage of payments authenticated though biometrics on a mobile device in the year 2014 is 15.13%. We arrive at this figure by taking the 83% of people who would choose to authenticate through biometrics out of the 68% of people who had devices with biometric capabilities out of the total percentage, 26.8%, of mobile electronic payments. Then, in order to arrive at the quantitative amount of money in transactions authenticated through biometrics via mobile devices in 2014, we take 15.13% of the total $51 billion (Statista, 2015)

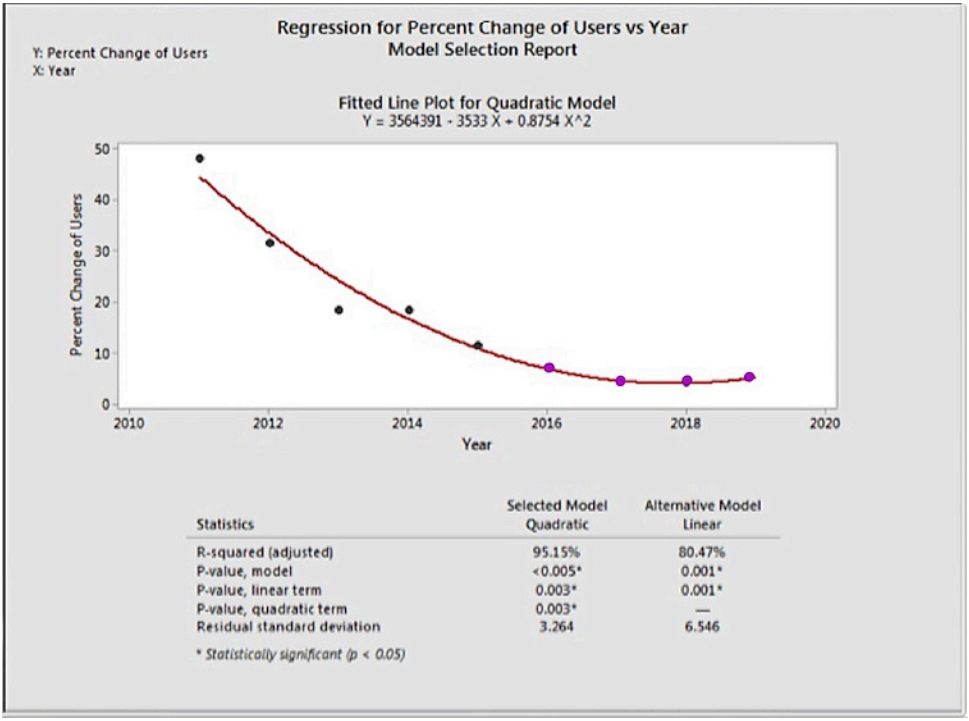

FIGURE 3: **This trend line was created through a regression analysis of the percent change in users of biometrics each year using the program Minitab.** The line's negative slope indicates that users of biometrics are increasing at a slowing pace, which reflects the stabilizing that occurs in the rate of a logarithmic function as it approaches its asymptote. Once again, a logarithmic model would be more realistic than the quadratic equation, however the available software did not support that option.

spent on transactions made through mobile devices to get $7.72 billion.

To move from the amount of money made through mobile payments authenticated via biometrics in 2014 to the subsequent years, we must determine the rate of change. In order to do so, a second regression analysis was created, pictured above in Figure 3. The red line shows the trend in the percent change of users over time, based on the data found in Figure 1, calculated by the equation ; wherein *y* is the number of users and is represented on the graph by a black dot. The purple dots represent the predicted values for the following years and therefore follow the trend line.

Assuming that each user's biometric transactions are the same amount of money on average, the percent change in biometric users is assumed to correlate directly to the amount of money spent in biometrically authenticated transactions. Thus, we are able to take the projected percent increase in users as determined in Figure 3 and apply them to the previous year's estimated amount of money made though mobile payments authenticated via biometrics in order to obtain to next year's amount and so on. The following table visually demonstrates the projected increase in money made through mobile

	2014	2015	2016	2017	2018	2019
Money made through mobile payments authenticated through biometrics	$7.72 billion	$8.60 billion	$9.18 billion	$9.64 billion	$10.02 billion	$10.26 billion
	11.40% →	6.80% →	4.98% →	3.96% →	2.34% →	

TABLE 2: **This table serves to show the yearly percent change in the increase of money made through mobile payments authenticated via biometrics.** The first cell follows from the last cell in Table 2 and each consecutive cell increases by the percentage indicated over the blue arrow. These percentages were derived from the percent change in biometric users, shown in Figure 3, which we assume directly correlates to the percent change in the money spent in biometrically authenticated transactions.

transactions that were authenticated using biometrics over the years.

As seen in Table 2 above, following the successive percent increase rates, in the year 2019 we arrive at the figure $10.26 billion as the quantity of money made through biometrically authenticated mobile transactions.

FUTURE APPLICATIONS

As a very versatile technology, which is projected to grow, there are many avenues through with biometrics can be implemented. One such way to make use of biometric systems is to employ them in universities to identify students for exams.

Currently, the common protocol for large classes across universities requires students to bring an identification card to prove they are a student enrolled in the class. Though this process works for the most part, there are a few major gaps in its functionality, which can be solved by replacing it with a fingerprint scanner. For instance, while ID cards are easy to lose or forget, the same cannot be said of fingerprints. An increase in security would result since those enrolled in the class would not be denied access solely because they do not have their identification on them, effectively increasing true matches. Additionally, it would provide an extra layer of protection, as it is much harder to impersonate someone when checking fingerprints.

However, as aforementioned, there are some limitations which could lead to false negatives that could lead to incorrect accusations of cheating, a major issue. Thus, in the beginning stages, it would be advisable to implement a backup system of identification to supplement the biometrics in case of a failure or any inaccuracies, however, as time goes on and biometrics becomes more sophisticated and the standards solidify, it will become more reliable.

CONCLUSION

As biometric technology becomes increasingly useful in everyday life, it is vital to evaluate its social acceptance and the associated privacy/security issues. According to our findings, in the coming years the number of biometric users will increase, thus it would be prudent to invest in biometrics by not only implementing more systems, but also making better, more reliable systems relying on new standards that are sure to follow.

ACKNOWLEDGEMENTS

Loren Barcenas was supported by the College of Science Research Seed Grant. Additional thanks go to Dr. Koray Karabina for his continual support and mentorship, as well as the FAU Office of Undergraduate Research and Inquiry for providing opportunities to present this research.

REFERENCES

Boulgouris, N., Plataniotis, K. N., & Micheli-Tzanakou, E. (2009). *Biometrics: Theory, Methods and Applications*. Hoboken, New Jersey: John Wiley & Sons.

Brandan, R. (2015). US Customs is Testing Out Biometric Scanners at Airports and Border Crossings. *The Verge*. Retrieved from http://www.theverge.com/2015/3/19/8259591/us-customs-iris-scanners-airports-border-fingerprint-biometric

Cheng, R. (2014). Apple, Samsung own two-thirds of US smartpones market. *CNET*. Retrieved from https://www.cnet.com/news/apple-samsung-own-two-thirds-of-us-smartphone-market/

Chowdhry, A. (2014). MasterCard And Zswipe Unveil Credit Card with Fingerprint Scanner. *Forbes*. Retrieved from http://www.forbes.com/sites/amitchowdhry/2014/10/18/mastercard-zwipe-fingerprint-sensor-credit-cards/#2cdbfd096be1

FIDO Alliance. (2015). About the FIDO Alliance. *FIDO Alliance* Retrieved from https://fidoalliance.org/about/overview/

Gerdeman, D. (2012). India's Ambitious National Identification Program. *Harvard Business School*. Retrieved from http://hbswk.hbs.edu/item/indias-ambitious-national-identification-program

Harwell, D., & Nakashima, E. (2015). China Suspected in Major Hacking of Health Insurer. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?utm_term=.a991b0ddf627

Humer, C., & Finkle, J. (2014). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved from http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Hussain, A. (2015). Are Mobile Payments Headed Towards Biometrics and the Cloud? [Web log comment]. Retrieved from http://blog.m2sys.com/mobile-biometrics-2/mobile-payments-headed-towards-biometrics-cloud/

Imprivata, Inc. (2014). Biometrics Healthcare. *Imprivata*. Retrieved from https://www.imprivata.com/biometrics_healthcare

internet Retailer. (2015). US E-Commerce Sales, 2014 - 2018. *Internet Retailer*. Retrieved from https://www.internetretailer.com/trends/sales/us-e-commerce-sales-2013-2017/

Jain, A. (2012). Biometric Authentication: System Security and User Privacy. *Identity Sciences, 45,* 87-92. doi:10.1109/MC.2012.364

King, R. (2013). Mobile commerce will drive millions of biometric smarphone shipments, billions in transaction. *Biometric Update*. Retrieved from http://www.biometricupdate.com/201309/mobile-commerce-will-drive-millions-of-biometric-smartphone-shipments-billions-in-transactions

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. London: Springer-Verlag.

Martinez-Diaz, M., Fierrez-Aguilar, J., Alfonso-Fernandez, F., & Ortega-Garcia, J. (2006). *Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification*. Madrid, Spain: IEEE.

Miltgen, C. L., Popovic, A., & Oliveria, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Elsevier*, *56*, 103-114. http://dx.doi.org/10.1016/j.dss.2013.05.010

National Health Care Anti-Fraud Association. (2015). The Challenge of Health Care Fraud. *National Health Care Anti-Fraud Association*. Retrieved from https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx

Osborne, C. (2015). Health Insurer Anthem Hit by Hackers, up to 80 Million Records Exposed. *ZD Net.* Retrieved from http://www.zdnet.com/article/health-insurer-anthem-hit-by-hackers-up-to-80-million-records-exposed/

Otto, G. (2015). OPM: Stolen Biometric Data List Grows by 4.5 Million. *FedScoop*. Retrieved from http://fedscoop.com/opm-breached-biometric-data-list-grows-by-4-5-million-people

Revilla, A. (2015). Samsung launching Biometric Mobile Pay Service in Korea. *Digital Trends.* Retrieved from http://www.digitaltrends.com/android/samsung-biometric-mobile-pay/

Sadowski, B. (2015). Are Biometrics the Next Big Thing in Payments? *Mobile Payments Today*. Retrieved from https://www.mobilepaymentstoday.com/articles/are-biometrics-the-next-big-thing-in-payments/

Sanger, D. (2015). Hackers Took Fingerprints of 5.6 million U.S. Workers, Government Says. *The New York Times*. Retrieved from http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html?_r=0

Seals, T. (2014). Apple Pay's Biometrics Open a New Security Era for M-Payments. *Tech Zone 360*. Retrieved, from http://www.techzone360.com/topics/techzone/articles/2014/10/22/391937-apple-pays-biometrics-open-new-security-era-m.htm

Shen, D. (2015). Attacking Your Trusted Core: Exploiting Trustzone on Android. *Black Hat USA*. Retrieved from https://www.blackhat.com/docs/us-15/materials/us-15-Shen-Attacking-Your-Trusted-Core-Exploiting-Trustzone-On-Android-wp.pdf

Shih, G. (2013). Facebook admits year-long data breach exposed 6 million users. *Reuters*. Retrieved from http://www.reuters.com/article/net-us-facebook-security-idUSBRE95K18Y20130621

Statista. (2015). Mobile payments in the United States from 2014 to 2019, by segment (in million US dollars). *Statista*. Retrieved from https://www.statista.com/statistics/312492/mobile-payments-in-the-united-states-by-segment/

Statista. (2014). Mobile commerce spending as percentage of total e-commerce spending in selected global markets in 2015, by device. *Statista*. Retrieved from https://www.statista.com/statistics/281256/mobile-commerce-as-percentage-of-e-commerce-sales/

Statista. (2015). Number of Facebook Users in the United States from 2013 to 2019 (in millions). *Statista*. Retrieved from https://www.statista.com/statistics/408971/number-of-us-facebook-users/

Stephans, J. (2014). Apple app opens new world of biometric banking. *USA Today*. Retrieved from http://www.usatoday.com/story/money/personalfinance/2014/06/29/banking-apple-biometric/11504139/

Sternstein, A. (2015). After OPM Debacle, Three-Step Biometric ID Checks are Coming. *Next Gov*. Retrieved from http://www.nextgov.com/cybersecurity/2015/06/after-opm-debacle-three-step-biometric-id-checks-are-coming/115132/