HADMÉRNÖK
BIZTONSÁGTECHNIKA

15. évfolyam (2020) 3. szám 5–16.
DOI: 10.32567/hm.2020.3.1

Kata Rebeka Szűcs,[1] Arnold Őszi,[2]
Tibor Kovács[3]

Mobile Biometric Solutions from Big Tech Companies

Nagyobb gyártók megoldásai mobil biometrikus azonosításra

Mobile and smart devices have become essential part of our lives, and as we use them a lot, they hold a huge amount of valuable data about us, which has to be protected. A popular way of protection, among others, is biometrics. In the following article we are introducing how mobile biometrics work, how biometric data is handled and protected on our phones, and why is it important to store it safely. We also conducted a study, asking non-corporate users about their thoughts, opinion and usage of mobile biometrics and its perceived safety.

Keywords: biometric authentication, biometric data, data protection

A mobil és okos eszközök mindennapi életünk részévé váltak, és mivel rengetegszer használjuk őket, óriási mennyiségű értékes adatot tárolnak rólunk, amelynek védelemre van szüksége. Ennek egy népszerű módja a biometria alkalmazása. A következő cikkben az okostelefonokon használt biometria működését, a biometrikus adatok kezelését és védelmét vizsgáljuk, kitérve arra, hogy miért fontos a biometrikus adatok biztonságos tárolása. Egy kérdőíves kutatást is készítettünk, amelyben a nem vállalati felhasználók véleményét kérdeztük a mobil biometria használatáról és az azzal kapcsolatos biztonságérzetről.

Kulcsszavak: biometrikus azonosítás, biometrikus adat, adatvédelem

[1] Óbuda University, PhD Student, Doctoral School on Safety and Security Sciences, e-mail: szucs.rebeka@phd.uni-obuda.hu; ORCID: https://orcid.org/0000-0002-2965-6295

[2] Óbuda University, Adjunct Professor, Bánki Donát Faculty of Mechanical and Security Technology Engineering, e-mail: oszi.arnold@bgk.uni-obuda.hu; ORCID: https://orcid.org/0000-0001-5988-0143

[3] Óbuda University, Associate Professor, Bánki Donát Faculty of Mechanical and Security Technology Engineering, e-mail: kovacs.tibor@bgk.uni-obuda.hu; ORCID: https://orcid.org/0000-0001-7609-9287

Introduction

Mobile and smart devices have become to a great extent part of our lives recently. We work, communicate and relax with them, which means that they hold an enormous amount of valuable data about us. This data has to be protected. Biometrics are a fashionable way to keep data safe, and this technology is available for smart devices, such as phones and tablets. The biometric market is growing rapidly, so the topic is relevant and worth examining. According to study by Spiceworks, nearly 90% of businesses will implement biometric authentication by 2020. In the same study, they found that fingerprint and face scanners are the most commonly known and used types in the corporate field, but generally it is visible that users miss transparency.[4] These methods are also very popular among non-corporate users, but the lack of certainty regarding data security and protection is also present among them. In the following article we aim to introduce how mobile biometrics work, how biometric data is handled and protected on our phones, and why it is important to store it safely. We also conducted a survey, asking non-corporate users about their thoughts and usage of mobile biometrics.

Mobile biometrics

Biometric identification is an automated technique which measures and records the individual physical and behavioural characteristics of a person and uses them for identification and authentication purposes.[5] There are two kinds of biometrics: physical and behavioural. The most popular ones from the physical category are fingerprint, iris and face. The most popular behavioural are voice, handwriting and walking.

The process of biometric authentication in general consists of two main parts. The first stage is the registration of the biometric feature of the user, and the digitisation and saving of this information. The second part is the authentication itself, when the system takes a new sample and compares it to the database. If the two samples match, the access is granted.[2] In other words, these are the enrolment and recognition phases.[6] During this process, a registered biometric is essentially a piece of computer code (can be binary, sting or an image) which is used as a reference in the future. The first part can be highly regulated within organisations, so when the sample is taken the owner's claimed identity can be verified. But in the second phase, the original identity is not challenged, the system is only looking for a match with the existing data, which means that the idea that biometrics are more secure in themselves than other methods is not correct. One important difference is that unlike passwords for example, biometrics do not require an exact match, the two samples

[4] 'Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology by 2020, '*Spiceworks,* 12. 03. 2018. Available: www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/. (20. 07. 2019.)

[5] Tibor Kovács, István Milák and Csaba Otti, *A biztonságtudomány biometriai aspektusai* (Pécs: Magyar Hadtudományi Társaság, 2012).

[6] ,Anil K. Jain, Arun A. Ross and Karthik Nandakumar, *Introduction to Biometrics* (London: Springer, 2011).

are compared for resemblance. The systems can be set to accept a reasonable level of certainty, which is secure enough but also able to recognise the user if for example their hands are too wet or dry. The acceptance level is called biometric matching threshold (measuring how the live and stored samples are alike). This is usually set lower than 100% to flexibly recognise these different states of the same bodypart, however, we have to keep in mind that lowering the threshold can also lower security levels. Another example is when the database is huge, it is better to set the threshold to a higher percentage, so we don't create several false positives by accepting prints which are similar, but are from two different people.[7] There are several body parts which can be used for biometric identification, however, in this paper we are only going to examine the ones used for mobile devices. It is also important to mention that biometric features of a person can change over the years, so the registered sample has to be updated from time to time.

Mobile biometrics means the implementation of biometric authentication on mobile devices such as smartphones and tablets. These are the available methods:

- fingerprint recognition
- face recognition
- iris recognition
- voice recognition.

Fingerprint recognition is based on the patterns of ridges and valleys of fingerprints, which are considered unique for every people. Fingertips can have more than a hundred characteristic features. The individual has to provide their fingerprint first, so it can be saved in the system, and during the authentication the new template can be compared to the existing template. This technology is used frequently.

Face recognition is based on the characteristics of the individual's face. This is popular, because cameras are inexpensive and are already implemented in smartphones. They do not require direct contact with the sensor. The biggest challenge in this method is that the face can vary a lot, shadows under the eyes, different hairstyles, glasses or beards have to be acceptable, but the system has to remain secure at the same time. If the acceptance threshold is lower, liveness detection can be applied (not just for this method), which means that the algorithm can recognise if a sample trying to access the system is a real, living person or just a replica, photo or sculpture with which somebody is trying to access without right.[8]

Iris recognition is one of the best methods of authentication as the chances of two irises being identical are significantly low. It is also easy to verify if the subject is live because of the pupil reflexes. The method is based on the analysis of the coloured ring of tissue around the pupil with infrared light. (We must note that iris and retina recognition are not the same, the latter uses the vascular network at the back of the eye for sampling. This can vary more than the iris pattern during the individual's life.)[9]

[7] Julian Ashbourn, *Biometrics in the new world* (Berkhamsted: Springer, 2014).

[8] Liam M. Mayron, 'Biometric Authentication on Mobile Devices,' *IEEE Security & Privacy* 13, no 3 (2015). Available: https://ieeexplore.ieee.org/document/7118088. (20. 03. 2019.)

[9] Kovács, Milák and Otti, *A biztonságtudomány.*

The last point of this list is the voice recognition, which is currently not really used in mobile phones. The problem with behavioural biometrics is that they can vary a lot per user as well, so they are more difficult to be used. Voice recognition can be a good example of this. Some smartphones have built in voice recognition, for example Siri in iPhone, but they are not sophisticated enough yet to be used for authentication. There can be many disturbing things in the environment (background noise, acoustics of the room) which make this technique hard to utilise for identification. Combining this with a pass phrase can improve security. On some online forums, there are stories that even though iPhone recognises for example 'Hey Siri' when its owner says it, it can also be fooled. Rarely, it allows others into the system if their voices are similar to the owner's (for example if the owner's sibling from the same sex is trying to access).

In mobile biometrics in general, most of these methods are easy to implement in smart phones and tablets as they already have the necessary sensors (for example camera or microphones), the computing power and storage in most cases.

Biometric authentication is very convenient as we can just use our body parts which are always with us, we do not have to remember and type in difficult PINs or passwords, and we do not have to have our badges with us. The main disadvantage though is that they cannot be or are much more difficult to be changed. Once they are compromised, misused, they cannot be used again, so the systems which are using biometrics require a higher level of security, more advanced or new methods of protection.

Biometrics can be most effective if they are used combined with other methods of authentication.

Solutions from big players

'As with any data, biometric information is only as secure as the system that protects it. There is nothing inherent in raw biometric data that makes it more secure. However, if it is stolen, it can be very difficult to use.'[10] As stated previously, if biometric data is stolen, the consequences can be more serious, so the data itself, which is going to be compared to the sample during authentication, has to be saved in a secure place. Threats in case of biometric authentication can target the biometric data itself, not just the system it is protecting. In this section, we are going to present the key players' solutions for mobile biometrics and securing biometric data.

Apple

The available methods of biometric authentication for Apple iPhones are using fingerprint and face recognition, and they are called Touch and Face ID.

[10] Fred O'Connor, 'How Secure Is Biometric Data?' *Veridium*, 11 July 2018. Available: www.veridiumid.com/blog/how-secure-is-biometric-data/. (15. 03. 2019.)

According to Apple, ‘the probability that a random person in the population could unlock your iPhone is 1 in 50,000 with Touch ID or 1 in 1,000,000 with Face ID.’ They also mention that for children whose characteristic features are not fully developed or for siblings and twins who look alike, these numbers can decrease significantly.[11]

Touch ID allows the users to unlock their phones with their fingerprints instead of passcodes. It can also authorise purchases from the App Store, iTunes Store, Apple Pay and Apple Books. Touch ID allows the user to try to access unsuccessfully only five times, after it, it requires a password or passcode (depending on the device type). A password is also required for the setup and modification of this function (and in some other cases). The button which makes the use of Touch ID possible is made of sapphire crystal, which protects the sensor and acts as a lens to help it focus on the finger. This is surrounded by a capacitive steel ring which detects touch and tells the reader to read the fingerprint. The sensor takes a high resolution picture of the fingerprint and the sub-epidermal layers of the skin. After this, a mathematical representation is created of the image and it is stored (never the image itself) and compared to the new enrolled samples.[12] The technology is constantly learning more about the user’s fingerprint, it expands the fingerprint map as additional overlapping parts are added when users try to access using different angles of their prints.[13]

The mathematical representation of the fingerprint image is well protected (and it is also impossible to reverse or engineer the original fingerprint from it or identify the user). It is stored in the chip in the device, which has an advanced security architecture, Secure Enclave, developed for the safe storage and protection of biometric and passcode data. The fingerprint data is encrypted, it is stored on the device, and protected with a key only available to the Secure Enclave. The saved fingerprint data is used only by Secure Enclave when it verifies if the enrolled new sample matches the saved one, and it cannot be accessed by any applications or the operating system either. As stated previously, this data is only stored in the chip itself, and it is not uploaded to the Apple servers, iCloud or anywhere else where it can be used to verify the user’s identity outside their phone.[14]

After the print is read, the processor forwards the data to the Secure Enclave. This process is also encrypted and authenticated with a session key using a shared key which is different for every Touch ID. The read image is only temporarily stored in the encrypted Secure Enclave and after the comparison it is discarded.

Face ID makes unlocking the phone possible just by looking at it. It can provide a robust authentication and a low false acceptance rate. It is using the TrueDepth camera which is able to recognise the face when activated (the phone is raised or the screen is touched). It is also able to recognise the intent, which means that the user has to look at it directly and their eyes have to be open. Once attention

[11] Alex Mathew, ‘Subtlety is the Future of Biometric Authentication,’ 4 October 2018. Available: www.counterpointresearch.com/subtlety-future-biometric-authentication/. (23. 03. 2019.)

[12] ‘About Touch ID advanced security technology,’ Apple Inc., 2017. Available: https://support.apple.com/en-bn/HT204587 (23. 03. 2019.)

[13] Ibid.

[14] Ibid.

is confirmed, the camera projects and reads more than 30 thousand infrared dots to create a depth map and a 2D infrared picture of the face. These images are also saved within the Secure Enclave as mathematical representations and the matching is also performed in this part of the chip. As faces can vary a lot per person as well, it is worth mentioning that Apple worked a lot to develop this feature using a variety of testers from several ethnicity, age group and so on, and their sensors are also able to recognise users in hats, glasses or with beards. Because of the infrared sensors it can also be used in brightness or total darkness. Face ID can be utilised like Touch ID for purchases.[15] Users can also use Touch or Face ID with third-party applications, in which case the app is only notified if the authentication by these is successful or not, they cannot access the data which is being compared.

Android, Google

Without going into device specific details, let us examine Google's solution. There is a separated area in the phone's hardware called Trusted Execution Environment (TEE), which works with a similar logic as Apple's solution, and where the capturing and recognition of the fingerprint happens. A TEE can either use its own processor and memory or it can use a virtualised instance of the main CPU. It is fully insulated and isolated and cannot be accessed. Trusty TEE, also known as Trusty OS, is the operating system for TEE, which allows it to communicate with the system. After the fingerprint is read, the Trusty OS checks the data inside the TEE and creates a set of validation data and an encrypted template, which both look like junk data to anything except the TEE.

The encrypted print data can be stored in the TEE or on the device's encrypted storage. The validation data is stored in the TEE only. Google requires the fingerprint templates (processed versions of raw images) to be cryptographically authenticated. The template is using software based encryption which is sensitive to device, user and time, so if any of those change or removed, it cannot be used again. This kind of data is not stored on Cloud or anywhere else and is not shared with any application (just the verification if the identification was successful or not.) In case of rooting of a device, fingerprint data is accessible.[16] The user can use this kind of authentication for payments here as well.

While we are discussing Android solutions, we will mention Samsung, who is also using this OS and is one of the main players in this industry. Samsung Pass represents the latest security developments at the firm. It 'is an »identity management as-a-service«, enabling secure access through biometric authentication', using fingerprint, iris and face recognition instead of passwords, passcodes and PINs.[17] Let us consider Samsung's one of the latest phones, Galaxy S10 as an example for Android. It has

[15] 'Apple's Face ID: An insider's guide,' TechRepublic, 2017. Available: www.techrepublic.com/resource-library/whitepapers/apple-s-face-id-an-insider-s-guide-free-pdf/ (23. 03. 2019.)

[16] Jerry Hildenbrand, 'How does Android save your fingerprints?' *Androidcentral*, 26 Sept. 2017. Available: www.androidcentral.com/how-does-android-save-your-fingerprints. (23. 03. 2019.)

[17] 'Samsung Pass,' *Samsung.* Available: www.samsung.com/uk/apps/samsung-pass/. (23. 03. 2019.)

an innovative on-screen Ultrasonic Fingerprint Scanner, which is able to read the 3D contours of the physical thumbprint, not just a 2D image of it, which enhances safety and increases recognition rate.[18] Interestingly, but not surprisingly, the implementation of this on-screen fingerprint recognition technology was initiated based on customer research. It showed for example that authentication with fingerprint is the most utilised method and that when the sensor is located on the front of the phone, it is considered more convenient, but at the same time it turned out that for users larger display is also important (so the sensor has to take as little space from the screen as possible). So in this case, Samsung is not using an optical sensor, but the ultrasonic version which uses ultrasonic wave to capture the uniqueness of the print. (The company uses machine learning to help the system recognise spoofing attempts as well to improve safety.)[19]

GDPR – a side note

Before we move on to our own research, we would like to mention GDPR shortly. General Data Protection Regulation, which came into force in May 2018, aims to protect data, to make data handling more transparent and to give data subjects (whose data is being handled) more control over their personal data. According to GDPR, biometric data belongs to the group of special categories of personal data, which means that it is forbidden to process this kind of data without the owner's clear consent and a lawful justification of using this kind of data.[20] Compliance can also be a risk factor for organisations, however, different than the rest of the categories which were mentioned above. If they fail to comply, they can be fined, up to 4 per cent of annual global turnover or twenty million euros, whichever is greater, and obviously there is also a risk of good reputation which can be strongly and negatively influenced by such incidents.[21]

Survey

To understand the local situation, we conducted an online survey with nine questions (plus demographics). We managed to collect 224 answers: 66% of them from males, 34% from females. 53% of the respondents live in Budapest and 40% live in a city in the countryside, so most of the responses came from cities and only 8% from elsewhere. A little more than half of the respondents (54%) are university students, the rest already work (only 9% of them are in a leader position). Also more than half

[18] 'Samsung Raises the Bar with Galaxy S10: More Screen, Cameras and Choices,' *Samsung.* Available: https://news.samsung.com/global/samsung-raises-the-bar-with-galaxy-s10-more-screen-cameras-and-choices. (23. 03. 2019.)

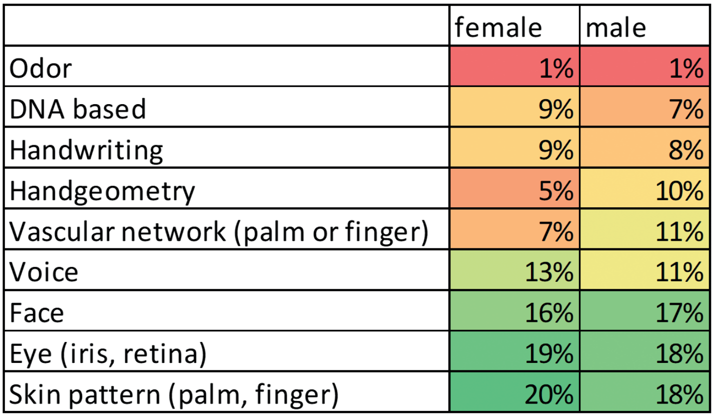
[19] Jennifer Langan, 'Ultrasonic Unlock: The Innovation Behind Our In-Display Fingerprint ID,' *Samsung.* Available: https://insights.samsung.com/2019/02/25/samsung-ultrasonic-fingerprint-scanner-how-why/. (23. 03. 2019.)

[20] Jeremy Dunn, 'Managing Biometric Data: The GDPR's Requirements,' *InfoToGo* 2018. Available: www.infogoto.com/managing-biometric-data-the-gdprs-requirements/. (05. 05. 2019.)

[21] 'GDPR Key Changes,' *EU GDPR,* 21. 04. 2018. Available: https://eugdpr.org/the-regulation/. (04. 05. 2019.)

of them (54%) has a graduation certificate, one third (35%) of them have finished college or university. In summary, we can see that the sample in average is relatively young, only 3% are Baby boomers (1946-1964), 13% are generation X (1965-1979), 33% are generation Y (1980-1994) and 50% belong to generation Z (born 1995-2010). All of the above mentioned features can influence the results of the survey which cannot be considered representative. This is an important differentiation, because these groups were at dissimilar ages when new technologies, such as smart phones, internet and biometrics became this widespread, which means they reacted differently and they feel differently about this new situation.

The first question we are going to analyse was about which biometric identification methods are known by respondents. On the below table we can see that the fingerprint and palm print recognition (91%), eye based (88%) and face (83%) recognition are the most well-known, possibly because lately they are built in to smartphones and they are getting popular every day. Interestingly, for a test, we included a fake possibility, too, and noticed that 17 (8%) respondents said that they are familiar with muscle tone based identification, which shows that there might be some respondents who marked that they know a certain method, but are not really familiar with it. Using Pivot tables and frequency analysis, it is visible that the male respondents knew more types than the females. In summary it is visible that biometric solutions are known by both genders. While men are more confidently familiar with the popular kinds, women are likely to know more types, as can be seen from the chart. We can also see that there might be a certain amount of confusion around the possibilities this method can offer (see our fake solution result).



	female	male
Odor	1%	1%
DNA based	9%	7%
Handwriting	9%	8%
Handgeometry	5%	10%
Vascular network (palm or finger)	7%	11%
Voice	13%	11%
Face	16%	17%
Eye (iris, retina)	19%	18%
Skin pattern (palm, finger)	20%	18%

Figure 1

Biometric identification methods known by respondents, n=224

Source: made by the authors.

24% of the respondents do not use biometric identification in their everyday life. This means that this kind of technology still has a potential to grow and convince more users to join. 70% of the respondents use biometrics on their phone, so this was the most common answer, which is not surprising. Here they could also mark more than one answers, 17% uses biometrics in access control systems (at university or at work), and there were about one third (27%) who mentioned using other devices such as tablets or laptops.

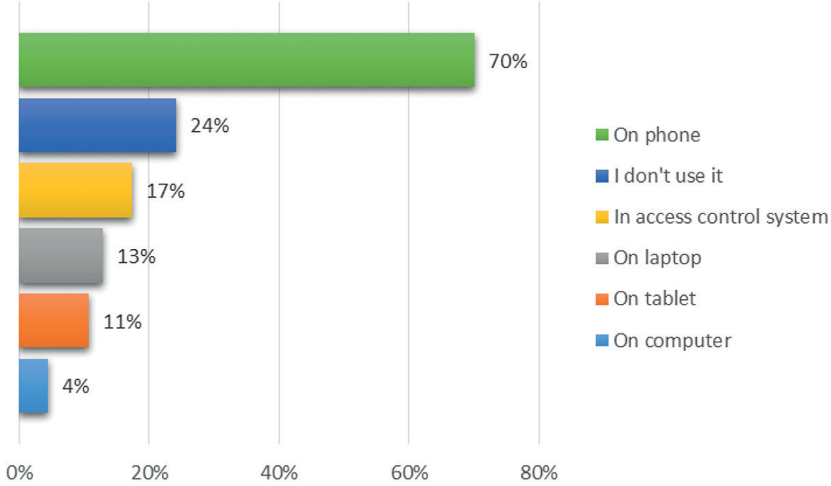


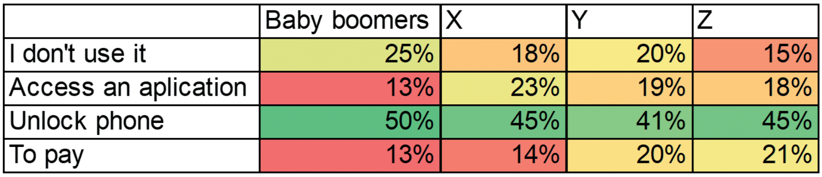
Figure 2

How do you use biometric authentication? n= 224

Source: made by the authors.

We examined these answers in relation to demographics using Pivot tables and we saw that if we consider gender, men are likely to use biometrics in more mobile devices than just on phones. This might be due to their stereotypical general interest for technology and technical gadgets. Here it is important to mention that 17% of the respondents said that their phone is not capable of biometric identification, which means that they might use it, but they cannot. However, there are some whose phone can deal with biometrics and they still do not use it anyway.

79% said that their phone is capable of processing fingerprint data, 33% can handle face recognition, 9% voice and 6% iris recognition. (This was also a question with more than one answer options.) Voice recognition is, as we mentioned, an interesting point, because they might be able to recognise the user's voice, however they are not accurate enough to be used for identification.



	Baby boomers	X	Y	Z
I don't use it	25%	18%	20%	15%
Access an aplication	13%	23%	19%	18%
Unlock phone	50%	45%	41%	45%
To pay	13%	14%	20%	21%

Figure 3

Usage of biometrics according to generations, n=224

Source: made by the authors.

We also queried what individuals use biometric identification on their phone for, which can be seen on Figure 3, in relation to generations. (Please note that the distribution percentages of subgroups are calculated per generations, that is, the columns.) Our assumption was that users who belong to younger generations are more likely to trust biometric solutions. We have found that more than two thirds (70%) confirmed that they use it to unlock their phone, we can also see from the table that this was the most popular answer for this point for all generations. Both accessing applications and verifying payments were chosen by around one third (30%). We can see that users from younger generations are more likely to pay with this method, which is considered to be more a private and delicate action, which backs up our initial expectation.

In the first part of the article, we mentioned that storing biometric data requires a higher level of security, as it is a special kind of data. We were curious where respondents think their biometric data is stored. This was also a multiple choice question and the results were the following (also visible in Figure 4): 76% think that their biometric data is stored on their phones' storage, which is generally the correct assumption. 41% of the respondents said that they thought their data is stored in the cloud, so some of them think their data is stored in both places. We could observe that this point is quite unclear for users, there were some additional comments here which supported this statement. This might mean for providers that a higher level of transparency about data storage and procession could raise the users' level of understanding and therefore trust in them.

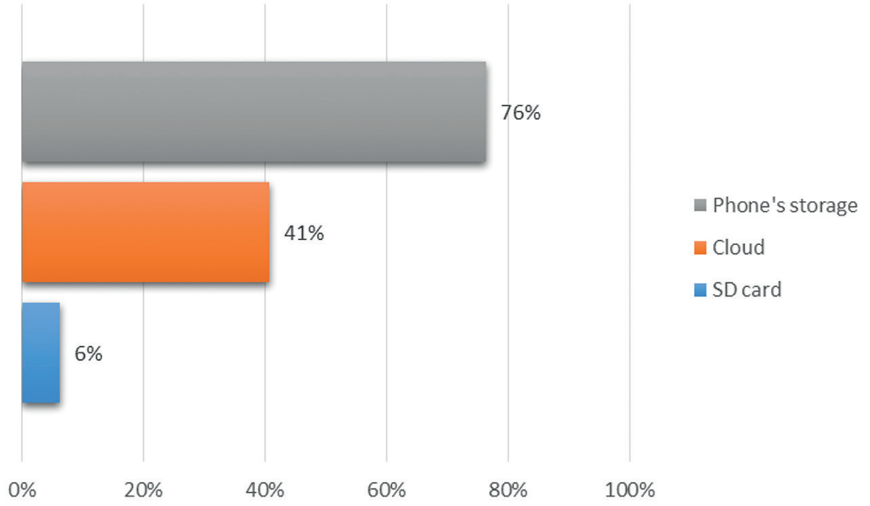
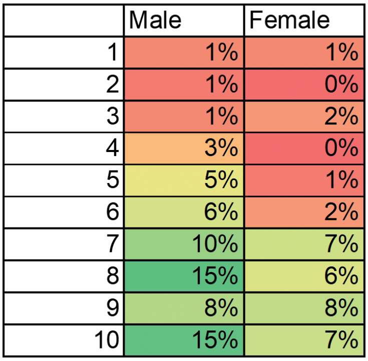


Figure 4

Where do you think your biometric data is stored for authentication? n=224

Source: made by the authors.

In the last section, we asked respondents about their approach to biometric identification, if they like or would like to use this method on a scale from 1 to 10 (1 equals never, 10 means always). The median of the answers was 9, the average was 7, which means that users in general are happy to use this method. If we consider gender, a higher percentage of men were comfortable with this method than women, which can mean that they are more knowledgeable about the subject. We also surveyed how safe they think biometric identification is (1 means not at all, 10 means that they trust it entirely). The median and average for this question were both 8, which means that they think this method is quite reliable. As Figure 5 shows, we could observe that male respondents are usually more positive about the safety of this method, but most of the female respondents trust it as well.



	Male	Female
1	1%	1%
2	1%	0%
3	1%	2%
4	3%	0%
5	5%	1%
6	6%	2%
7	10%	7%
8	15%	6%
9	8%	8%
10	15%	7%

Figure 5

Do you think biometrics are safe? n=224

Source: made by the authors.

Summary

Considering the growing popularity of smartphones and biometrics, we aimed to examine the topic of mobile biometric solutions from the ‘big players’ in the smart phone field. We started with a general overview of the methods and introduced the ways to secure our biometric data when it is used on mobile phones. (We have to remember that there are other risks as well, not just secure biometric data storage.) To get a picture of the current acceptance and view of biometrics around us, we conducted a survey as well. According to our sample, still a quarter of our respondents do not use biometrics in their everyday life, but it is getting popular. Those who use it however, mostly use it on their phones. Men tend to use biometrics on more types of devices compared to women. The main use of biometrics is to unlock smartphones, but one third of the respondents like to access applications with this data or to pay with it. We assumed that there is some confusion around how biometric data is stored on our phones, but three quarters of the respondents knew correctly, which means users are getting more conscious regarding data security. Generally we can see that biometric authentication is well liked by users and thought to be trustable.

In the future, our plan is to study mobile biometrics in more detail, with special attention to possibilities of secure biometric data storage and methods.

References

‘About Touch ID advanced security technology.’ *Apple Inc.,* 2017. Available: https://support.apple.com/en-bn/HT204587 (23. 03. 2019.)

‘Apple’s Face ID: An insider’s guide.’ TechRepublic, 2017. Available: http://www.techrepublic.com/resource-library/whitepapers/apple-s-face-id-an-insider-s-guide-free-pdf/ (23. 03. 2019.)

Ashbourn, Julian: *Biometrics in the new world*. Berkhamsted, Springer, 2014. DOI: https://doi.org/10.1007/978-3-319-04159-9

Dunn, Jeremy: ‘Managing Biometric Data: The GDPR’s Requirements.’ *InfoToGo* 2018. Available: www.infogoto.com/managing-biometric-data-the-gdprs-requirements/. (05. 05. 2019.)

‘GDPR Key Changes.’ *EU GDPR,* 21. 04. 2018. Available: https://eugdpr.org/the-regulation/. (04. 05. 2019.)

Hildenbrand, Jerry: ‘How does Android save your fingerprints?’ *Androidcentral*, 26 Sept. 2017. Available: www.androidcentral.com/how-does-android-save-your-fingerprints. (23. 03. 2019.)

Jain, Anil K. – Ross, Arun A. – Nandakumar, Karthik: *Introduction to Biometrics.* London, Springer, 2011. DOI: https://doi.org/10.1007/978-0-387-77326-1

Kovács, Tibor – Milák, István – Otti, Csaba: *A biztonságtudomány biometriai aspektusai*. Pécs, Magyar Hadtudományi Társaság, 2012.

Langan, Jennifer: ‘Ultrasonic Unlock: The Innovation Behind Our In-Display Fingerprint ID.’ *Samsung.* Available: https://insights.samsung.com/2019/02/25/samsung-ultrasonic-fingerprint-scanner-how-why/. (23. 03. 2019.)

Mathew, Alex: ‘Subtlety is the Future of Biometric Authentication.’ 4 October 2018. Available: www.counterpointresearch.com/subtlety-future-biometric-authentication/. (23. 03. 2019.)

Mayron, Liam M.: ‘Biometric Authentication on Mobile Devices.’ *IEEE Security & Privacy* 13, no 3 (2015). DOI: https://doi.org/10.1109/MSP.2015.67

O’Connor, Fred: ‘How Secure Is Biometric Data?’ *Veridium*, 11 July 2018. Available: www.veridiumid.com/blog/how-secure-is-biometric-data/ (15. 03. 2019.)

‘Samsung Pass.’ *Samsung.* Available: www.samsung.com/uk/apps/samsung-pass/. (23. 03. 2019.)

‘Samsung Raises the Bar with Galaxy S10: More Screen, Cameras and Choices.’ *Samsung.* Available: https://news.samsung.com/global/samsung-raises-the-bar-with-galaxy-s10-more-screen-cameras-and-choices. (23. 03. 2019.)

‘Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology by 2020.’ *Spiceworks,* 12. 03. 2018. Available: www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/ (20. 07. 2019.)