International Journal of Engineering & Technology, 7 (4.15) (2018) 491-495

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



A Survey of User Preferences on Biometric Authentication for Smartphones

Nur Syabila Zabidi[1]*, Noris Mohd Norowi[2]*, Rahmita Wirza O.K. Rahmat[2]

[1]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Selangor, Malaysia
[2]Faculty of Computer Science and Information Technology, Universiti Tun Hussien Onn Malaysia, Johor, Malaysia
**Corresponding author E-mail: gs45571@upm.edu.my, noris@upm.edu.my*

Abstract

The search for improving users' security needs, awareness and concerns in the context of mobile phones still has been conducting in today's society. Biometric systems identify a person or verify the identity of a person using purportedly unique physical traits or behaviour of that individual. In order to understand user requirements for biometric authentication, it is important to focus on several key issues, including the importance of smartphones in implementing biometric authentication, users' general knowledge and perception towards biometric authentication, and users' trust and practice when using different biometric technology for securing their smartphone's data. A preliminary study in the form of an online survey was conducted. The idea of this study was to conduct a survey on users about their general knowledge and perceptions towards different biometric authentication on smartphones. The results of the study indicate that smartphone is an important tool in implementing biometric authentication. Moreover, users knew what biometric technology is and they are not reluctant to use them. Furthermore, users knew how to protect their smartphone's data and practice the related preventions. The results are expected to give an insight of deploying biometric technology into mobile devices and further researching onto others biometric authentication.

Keywords: *Authentication; Biometric; Smartphones.*

1. Introduction

The growing number of smartphone users creates a situation for people to start worrying about their personal data. The privacy and security of an individual should be protected. People tend to store their personal information on their smartphones. Details about medical information, personal identifiers, or financial data can be stolen or misused. With this in mind, authentication plays an important role to help establish proof of identity.

The process used to verify the identity of a user is known as user authentication. In [1] categorized the authentication methods as knowledge-based (password/PIN), possession based (certificate/card) and biometric based (finger/iris scan/face). In the same manner, user authentication refers to the process in which a user submits his/her identity credential (often represented by pairing username and password) to an information system and validates to the system that he/she is who he/she claims to be [2]. Conventional password method increases frustration where users have to remember certain number of passwords [3]. Likewise, passwords do not provide compromise detection and do not offer much defence [4].

This study utilized smartphones as the platform of choice for implementing biometric-based authentication. According to the increasing mobile security of Internet users, many users are interested in biometric verification of personal identification and authentication in mobile security because over 75 percent of online users have experience of authentication failure by forgetting passwords, usernames or a response to a knowledge-based question [5].

Biometric techniques use unique physiological (e.g. face recognition), behavioural (e.g. signature), and a combination of physiological and behavioural features [6]. Biometric-based authentication can be divided into two modes: identification (Who owns this biometric?) and verification (Am I the person I claim to be?) [7].

The main motivations of this study consider the smartphones' abilities and the rise of biometric technologies. As it is more common for people to use smartphones daily, it is equally important to study what are the user requirements and preferences when implementing a biometric authentication on smartphones.

This paper studies user preferences on biometric authentication. The goal is to gather and analyse user requirements for the purpose of designing biometric features on smartphones. We focus on the general knowledge and perception towards the security and privacy of data.

The paper is organized as follows: Section 2 provides the related works of smartphones, user authentication, and biometric technology. Section 3 discusses state-of-the art technology of biometric authentication. Section 4 presents the study design of an online survey. Section 5, 6 and 7 presents the results, analysis, and discussion from an online survey. Finally, Section 8 concludes the work and highlights a direction for future research.

2. Related Work

2.1. Smartphones

Smartphones and mobile devices equipped with progressive sensors such as high-resolution cameras, digital compasses, gyroscopes, accelerometers, positioning systems provide a wide platform for researchers to enhance built in functions of these devices

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[8]. In [9] described smartphones as small, portable and powerful device that serve users with multiple task.
With the development of mobile devices and the 3G mobile network, smartphones have assumed an important role in our life. Mobile phones allow Internet surfing, website login, gaming, stock investing, etc. Meanwhile, due to their convenience, most people store their personal information in their mobile phone. Once the phone is stolen or lost, the information can be accessed for malicious purposes by others. In the situations stated above, developing a reliable authentication mechanism for mobile devices becomes an essential research issue.
According to [10] a manifold of sensitive user data has to be protected by implementing lock screen to verify the user's identity in smartphone. This statement is supported by [2] where they stated that it is very demanding in storing security information in mobile. In fact, to prevent any unauthorized accesses to the information, authentication becomes the most important elements in smartphones. For this reason, smartphones are chosen to be the suitable candidate to serve as a platform to implement biometric-based authentication [8].

2.2. User Authentication

In [1] described user authentication as a process to verify identity of a user. They categorized the authentication methods as knowledge-based (password/PIN), possession based (certificate/card) and biometric based (finger/iris scan/face).
The categorization of user authentication is further supported by the research work made by [11] where they divided also authentication into three different types, knowledge-based, token-based and biometric-based.
Based on these categorizations, we can conclude that knowledge-based authentication is something a user knows such as a password or PIN. On the other hand, possession-based or token-based authentication is something a user possess such as a certificate or card. While biometric-based authentication is something a user is such as iris scan, fingerprint and face recognition.

2.3. Biometric Authentication

To understand what biometric authentication is, in [1] has outlined the definition of biometric where the biometric system identifies a person uniquely by their physical traits or behaviour. It can be based on fingerprints, iris, facial images, voice, palm prints, keystroke dynamics, etc.
However, according to [11] biometrics are divided into two types; physical and behavioural. Physical biometric includes palm, fingerprint and iris recognition while behavioural biometric include the signature and keystroke dynamics.
This research utilized the characteristics of biometric to implement user authentication for smartphones. In [5] analyzed that many users are interested in using biometric authentication for their personal identification in smartphones. It is because over 75% of users having the experience of authentication failure where they seemed to forget their passwords or usernames. On the other hand, a frequently mentioned usability disaster stated by [3] is password expiration policies whereby it increases login errors and prevents users to log out from existing machines.
One of the biometric features that possible to be implemented is the recognition of smiles. Smile evaluation is basically performed by clinical means such as photographs and filming [12]. In [13] stated that every face has their own disproportions and asymmetries which means smile included in these key features. With attention to smiles, smiles include not only a stable configuration of features, but also temporally consistent movement patterns. In [14] studied portions of the smile display are relatively stereotyped and may be automatically produced. However, this study is limited by the only sample data tested, which is the right lip corner. The anatomy of a smile constituted by the normal curvature of the lips, the proper exposure of the red zone of the lips and the harmonious of the exposed teeth [15]. Portions of the smile display are relatively stereotyped and may be automatically produced [14].
Therefore, biometric technology is chosen to be the smartphones' authentication for this study. As biometric is potentially faster than entering a password, it is the easier way for user without needing to remember password and increase the possibility of creating login errors [16].

3. State-of-the-Art Technology of Biometric Authentication

Biometric features used in mobile devices are in global scale considering the usage of mobile in most human activities. The growing interest in their use for capturing and processing biometrics data is now heading towards the aim of user authentication.
Early work of [17] was concerned with Mobile Personal Device (MPD) in a Personal Network (PN) based on face biometric authentication method by using Viola-Jones detector. In [18] further upgraded their system by introducing five key modules: 1) face detection; 2) face registration; 3) illumination normalization; 4) face verification; and 5) information fusion which was able to achieve an equal error rate of 2%. Additional work by [19] deals with a systematically method in performance evaluation of different combinations of fusion methods and normalization techniques in different noise.
Several researchers addressed the issues of usability and security to be adapted to the successful authentication solutions. In [6] studied various aspects of these issues. They presented a concise survey on different types of biometric methods. In summary, they concluded to have a multimodal identity management system. In a report on a different case, in [20] has concluded that the technical challenges arise in image processing aspects such as bias lighting conditions and unstable sample collection environment. Three biometric authentication modalities; which is voice, face and gesture was developed by [21] on a mobile device to explore the relative demands on user time, effort, error and task disruption. The general results reflecting the unique strengths and weaknesses on each biometric modality. In the final analysis, they concluded that face and voice are fast but not universally usable. Moreover, a much shorter gesture would be needed to achieve a competitive time.
By considering usability and security as focus points on biometric technology, in [16] introduced pan shot face unlock as an approach to increase security and usability during mobile device authentication. The results stated that the approach to face recognition is sufficient for their research; yet face detection still needs to be further looked into. In a different study by [22] proposed a novel software-based liveness detection method, specifically for face, iris and fingerprint spoofing attack detection in mobile applications by employing a novel real-time feature description based on order permutations, named Locally Uniform Comparison Image Descriptor (LUCID).
While the above studies provide valuable information regarding the aspects of usability and security, cautions need to be focused on the impact of using mobile devices as terminals. With this intention, in [5] studied on recognizing the left and right facial profile images as well as the front facial images as a biometric verification of personal identification and authentication for mobile security. This study showed a robust result to change in illumination, face size and background noises. Additional work by [8] exploited smartphone's embedded sensors to capture both ear shapes (represented through LBP) and arm motion when responding or placing a call (represented through DTW) to achieve improved recognition accuracy by data fusion at score level.
In this paper, a survey was presented for obtaining the knowledge of usability and security issues. These issues are based on a series of users' preferences and specific assumptions towards biometric technology. However, this information is valid for a small range of real mobile device situations. The underlying assumptions of the survey are presented in the following section.

4. Study Design

In order to understand user requirements for biometric authentication, a preliminary study in the form of an online survey was conducted. The idea of this study was to survey the users about their general knowledge and perceptions towards different biometric authentication on smartphones. This study intended to see the users' willingness in adapting another biometric authentication. In this survey, a set of personal characteristics namely age, sex, education, average household income and smartphones ownership of the 77 respondents have been examined and presented.

4.1. Age

The most important characteristics in understanding users' views was the age of the respondents. Age is vital in examining the level of maturity of individuals in the responses. Table 1 shows that on an average, respondents were about 21 to 30 years of age with the standard deviation of 0.71. Nearly 2.6% were under 21 years of age, whereas 27% were above 31 years of age. To be more specific, large number of respondents were 30 years of age in the sample. Some interesting feature of this age of the respondents is that young respondents were widely exposed to the use of smartphones. This suggests that the use of smartphones is highly relevant to be the platform for studying biometric authentication.

Table 1: Age of the respondents

Answer Choices	Percentage	Number of Responses
Under 21 (1)	2.60%	2
21 to 30 (2)	51.95%	40
31 to 40 (3)	35.06%	27
41 to 50 (4)	10.39%	8
Over 50 (5)	0.00%	0
Total	100.00%	77

4.2. Sex

Table 2 shows that out of the total respondents investigated in this study, an overwhelming majority (74.03%) of them were females, whereas about 25.97% were found to be males.

Table 2: Sex of the respondents

Answer Choices	Percentage	Number of Responses
Female (1)	74.03%	57
Male (2)	25.97%	20
Total	100.00%	77

3. Education

Education is one of the most important characteristics that might affect the person's attitudes and the way of looking and understanding any particular social phenomena. In a way, the response of an individual is likely to be determined by his educational status and therefore it becomes imperative to know the educational background of the respondents. Table 3 shows that about 41.56% of the respondents were educated up to Master's Degree and relatively lesser number of them, 3.9% were educated up to secondary school. The number of respondents attaining higher education was also larger. It can be concluded from the Table 3 that by and large the respondents were progressive in education. These suggest that a knowledge based society indirectly helps in establishing unique biometric authentication.

Table 3: Education of the respondents

Answer Choices	Percentage	Number of Responses
Secondary School (1)	3.90%	3
Diploma (2)	14.29%	11
Bachelor's Degree (3)	28.57%	22
Master's Degree (4)	41.56%	32
Doctorate (5)	11.69%	9
Other (please specify) (6)	0.00%	0
Total	100.00%	77

4.4. Income

The income of a person plays an important role in shaping the economic conditions of an individual which in turn is likely to have responses on ownership of smartphones. From Table 4, it can be seen that most of the respondents (40.26%) were in the highest income group, whereas only 6 of them were in low income group. In [23] have concluded income inequality is due to differences in the income levels across ethnic groups in Malaysia. However, incomes show similar patterns (if different levels) for household groups, regardless of the ethnicity. Since the survey was conducted online, this suggests that regardless of respondents' income, the large majority still had access to the internet.

Table 4: Income of the respondents

Answer Choices	Percentage	Number of Responses
Below RM 999 (1)	7.79%	6
RM 1,000 to RM 1,999 (2)	2.60%	2
RM 2,000 to RM 2,999 (3)	12.99%	10
RM 3,000 to RM 3,999 (4)	16.88%	13
RM 4,000 to RM 4,999 (5)	19.48%	15
RM 5,000 and up (6)	40.26%	31
Total	100.00%	77

4.5. Smartphones Ownership

The possession of a smartphone is a normal situation in today's society. The smartphones ownership is likely to be the most needed properties of a person in using a variety of applications in daily life. The smartphones ownership is therefore likely to have an impact on the type of response given by the respondents and therefore the variable 'smartphones ownership' was considered an important variable and the data is presented in Table 5. Table 5 shows that all of the respondents (100%) had used and owned smartphones. It can therefore be concluded that smartphones are the basic needs in today's society which means that regardless of education and income status, smartphones are affordable to be bought.

Table 5: Smartphones ownership of the respondents

Answer Choices	Percentage	Number of Response
Yes (1)	100.00%	77
No (2)	0.00%	0
Total	100.00%	77

5. Importance of Smartphones

Mobile phone application development has taken a huge step from its first days of development on monochrome screens. There are three widely used development platforms for pervasive applications: 1) Android, a Linux based operating system from Google; 2) The Windows Phone operating system from Microsoft; and 3) The iOS platform from Apple [24].

Figure 1a shows the distribution of smartphone platform used by the respondents. The majority of the respondents were using the Android operating system (66.23%). The total time spent on using smartphones is shown in Figure 1b where 36.38% of the respondents used smartphones for 2 to 4 hours, while 8% respondents either use phones as minimum as 2 hours only or 8 hours and above. Based on these responses, it indicates that smartphones were very important in implementing biometric authentication. Smartphones are rapidly becoming a main computing platform for people to access personal information.

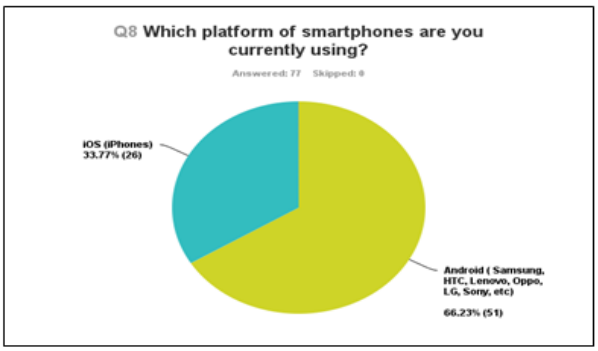


Fig. 1a: Demographics of smartphones platform.

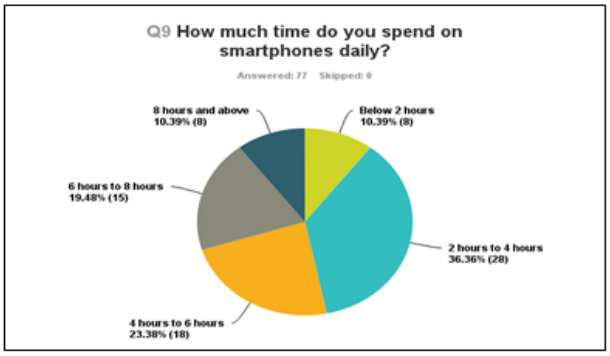


Fig. 1b: Demographics of smartphones usage.

6. General Knowledge and Perception towards Smartphones

It can be generally described that the general knowledge and perception towards the use of biometric among smartphone users in Malaysia are warmly received. For instance, almost all of the users (93.51%) surveyed reported to have used PIN or password method. This suggests that smartphone users were generally concerned and alert about the safety of the information stored on their smartphones. Surprisingly, more than half of these user surveyed (58.44%) revealed that they have used fingerprint technology as an alternative method to authenticate phone and further protecting personal information (see Figure 2a).

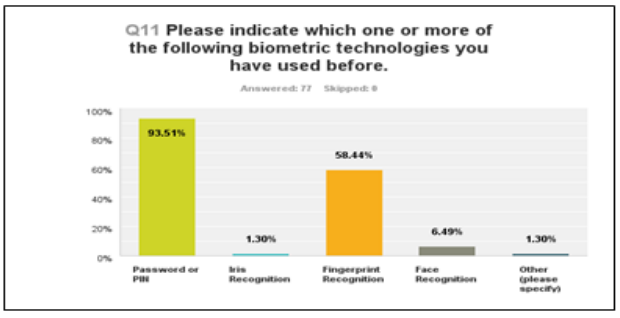


Fig. 2a: List of biometric technologies.

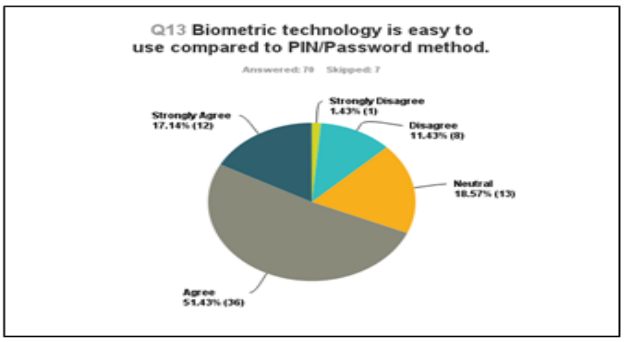


Fig. 2b: Easiness of biometric technologies.

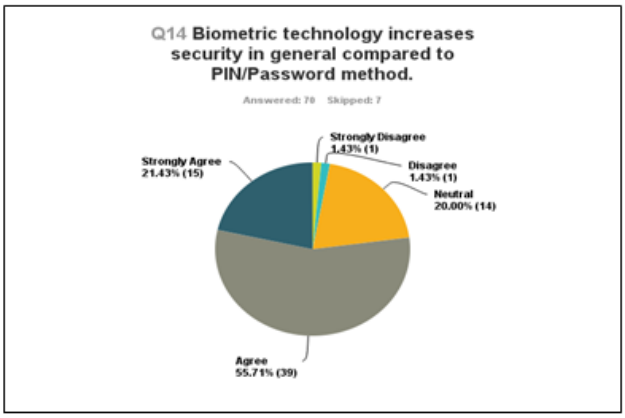


Fig.2c: Security of biometric technologies.

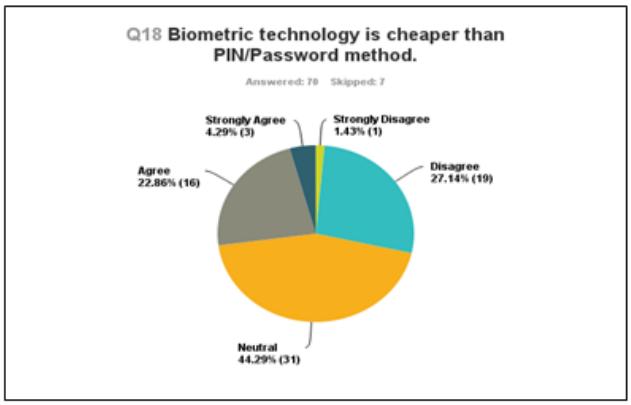


Fig.2d: Price of biometric technologies.

With the intention of gaining basic knowledge and perception towards biometric technologies, a list of statements requiring agreement of level were asked to the respondents. First, in terms of the easiness of biometric technology, 51.43% of the users agreed biometric technology is easy to use compared to PIN/Password method (Figure 2b). Second, by comparing to PIN/Password method, 55.71% of the users agreed biometric technology is more secure (see Figure 2c). However, 44.29% of the respondents seems to be neutral in agreeing the statement of biometric technology price. Surprisingly, there were 19 respondents disagreed biometric technology is cheaper that PIN/Password method (see Figure 2d).

Based on these results, it can be concluded that users knew what biometric technology is and agreed to use them. This also shows that Malaysian smartphone users are up-to-date with the current technology and are not afraid to embrace change.

7. Trustworth and Practices towards Biometric

The pie chart in Figure 3a shows how respondents rated the importance of data protection and security on smartphones. 72.58% of the respondents highly agreed to this statement. When they were asked which preferred method they will implement in protecting their smartphone's data, 32 respondents agreed to use Password/PIN and surprisingly, 31 respondents also preferred the use of fingerprint recognition method (see Figure 3b). There were also considerate percentage, of about 64.29%, knew how to protect their smartphone's data by always logging off from all related applications.

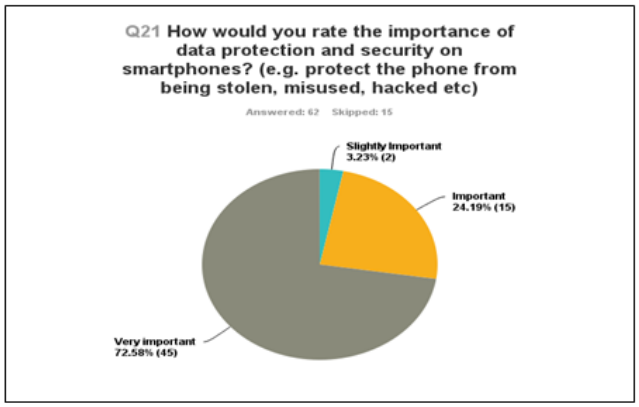


Fig. 3a: Importance of data protection and security on smartphones.

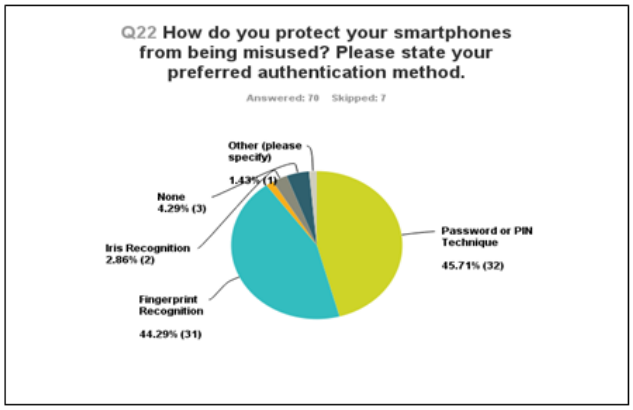


Fig.3b: Preferred authentication method.

Based on these results, it can be concluded that users knew how to protect their smartphone's data and practice the related preventions. It is therefore possible to implement biometric authentication by cultivating the knowledge of protecting users' personal information.

8. Conclusion

With the development of mobile devices and the 3G mobile network, smartphones have assumed an important role in our life. Mobile phones allow Internet surfing, website login, gaming, stock investing, etc. Meanwhile, due to their convenience, most people store their personal information in their mobile phone. Once the phone is stolen or lost, the information can be accessed for malicious purposes by others. In the situations stated above, developing a reliable authentication mechanism for mobile devices becomes an essential research issue.

In this paper, an online survey has been conducted to help identify the key characteristics of implementing a biometric authentication for smartphones. The results of the study were found to lean in favour towards the use of biometric authentication among smartphone users in Malaysia. In addition, this study also looked into the potentials of using other biometric authentication such as smile recognition in authenticating access to a users' smartphones.

References

[1] Srivastava, S., & Sudhish, P. S. (2016). Continuous multi-biometric user authentication fusion of face recognition and keystroke dynamics. Proceedings of the IEEE Region 10 Humanitarian Technology Conference, pp. 1–7.

[2] Li, Y., Yang, J., Xie, M., Carlson, D., Jang, H. G., & Bian, J. (2015). Comparison of PIN- and pattern-based behavioral biometric authentication on mobile devices. Proceedings of the IEEE Military Communications Conference, pp. 1317–1322.

[3] Herley, C., & Oorschot, P. V. (2012) A research agenda acknowledging the persistence of passwords. IEEE Security and Privacy, 10(1), 28–36.

[4] Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2020–2021.

[5] Jung, E., & Hong, K. (2015). Biometric verification based on facial profile images for mobile security. Journal of Systems and Information Technology, 17(1), 91–100.

[6] Mastali, N., & Agbinya, J. I. (2010). Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper. Proceedings of the 5th International Conference on Broadband and Biomedical Communications, pp. 1-6.

[7] Zirjawi, N. (2015). A survey about user requirements for biometric authentication on smartphones. Proceedings of the IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering, pp. 1–6.

[8] Abate, A. F., Nappi, M., & Ricciardi, S. (2016). Smartphone enabled person authentication based on ear biometrics and arm gesture. Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, pp. 3719–3724.

[9] Mayron, L. M. (2015). Biometric Authentication on Mobile Devices. IEEE Security and Privacy, 13(3), 70–73.

[10] Holz, C., Buthpitiya, S., & Knaust, M. (2015). Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 3011–3014.

[11] Liu, C. L., Tsai, C. J., Chang, T. Y., Tsai, W. J., & Zhong, P. K. (2015). Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. Journal of Network and Computer Applications, 53, 128–139.

[12] Machado, A. W. (2014). 10 commandments of smile esthetics. Dental Press Journal of Orthodontics, 19(4), 136–157.

[13] Duggal, S. (2012). The esthetic zone of Smile. Virtual Journal of Orthodontics, 9(4), 10–22.

[14] Schmidt, K. L., Cohn, J. F., & Tian, Y. (2003). Signal characteristics of spontaneous facial expressions: Automatic movement in solitary and social smiles. Biological Psychology, 65(1), 49–66.

[15] Matthews, T. G., Blatterfein, L., Morrow, R. M., & Payne, S. H. (1978). The anatomy of a smile. Journal of Prosthetic Dentistry, 39(2), 128–134.

[16] Findling, R. D., & Mayrhofer, R. (2013). Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices. International Journal of Pervasive Computing and Communications, 9(3), 190–208.

[17] Tao, Q. & Veldhuis, R. N. J. (2006). Biometric authentication for a mobile personal device. Proceedings of the 3rd Annual International Conference on Mobile Ubiquitous Systems - Workshops, pp. 6–8.

[18] Tao, Q., & Veldhuis, R. (2010). Biometric authentication system on mobile personal devices. IEEE Transactions on Instrumentation and Measurement, 59(4), 763–773.

[19] Yuan, X., & Rahim, M. S. (2010). User authentication on mobile devices with dynamical selection of biometric techniques for optimal performance. Proceedings of the IEEE International Conference on Robotics and Biomimetics, pp. 333–338.

[20] Derawi, M. O. (2011). Biometric options for mobile phone authentication. Biometric Technology Today, 2011(10), 5–7.

[21] Trewin, S., Swart, C., Koved, L., & Martino, J. (2012). Biometric authentication on a mobile device: a study of user effort, error and task disruption. Proceedings of the 28th Annual Computer Security Applications Conference, pp. 159–168.

[22] Akhtar, Z., Michelon, C., & Foresti, G. L. (2014). Liveness detection for biometric authentication in mobile applications. Proceedings of the International Carnahan Conference on Security Technology, pp. 1–6.

[23] Saari, M. Y., Dietzenbacher, E., & Los, B. (2014). Income distribution across ethnic groups in Malaysia: Results from a new social accounting matrix. Asian Economic Journal, 28(3), 259–278.

[24] Gronli, T. M., Hansen, J., Ghinea, G., & Younas, M. (2014). Mobile application platform heterogeneity: Android vs windows phone vs iOS vs Firefox OS. Proceedings of the IEEE 28th International Conference on Advanced Information Networking and Applications, pp. 635–641.