How Users Perceive Authentication of Choice on Mobile Devices

Akintunde Jeremiah Oluwafemi
Computer and Information Sciences Department
Towson University
Towson, USA
e-mail: aoluwa2@students.towson.edu

Jinjuan Heidi Feng
Computer and Information Sciences Department
Towson University
Towson, USA
e-mail: jfeng@towson.edu

***Abstract*—When interacting with an application, users expect to complete the desired tasks securely with minimal interference from the actions required to ensure security and privacy. Previous research confirmed that there is a tradeoff between the security and usability of an application. Although numerous user studies examined various authentication methods, such as alphanumeric password, graphical password, and biometrics, very limited research investigated users' performance and perception when they were allowed to choose the authentication method(s) for a specific application. This study investigates how users interact with and perceive the 'authentication of choice' method when using a mobile device. 75 participants completed an online study that compared three different authentication designs: alphanumeric username and password, one-factor authentication of choice, and two-factor authentication of choice. The result of the study confirms the tradeoff between security and usability in the design of authentication mechanisms. The result also indicates that the 'authentication of choice' approach has the potential to offer a solution that provides the desired balance between usability and security.**

Keywords-Access control; Authentication of choice; Usability; Security.

I. Introduction

Security can be defined as the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or advertent unauthorized use, destruction, disclosure, or alteration [1]. With the continuous increase in security threats, it is crucial to incorporate security measures into the system design to ensure the security of both the system and the information that resides in the system. Authentication is the process of identifying an individual process or entity that is attempting to log in to a secure domain. One goal of authentication design is to ensure users can perform their primary tasks securely with minimal interference [2][3]. Previous research confirmed the tradeoff between the security and usability of common authentication methods currently in use. A particular measure that improves the security of the authentication mechanism usually has a negative effect on the usability of the system [4].

Due to the huge variation in the user abilities and preferences, the nature of tasks and devices, and the context of use, the authentication process should not be one-size-fits -all. An authentication method that is usable for a specific user in a particular context may not be usable for other users in another context. For the same reason, an authentication method that is considered by some users to be sufficiently secure may not be secure enough for other users. When choosing an authentication method, the user's preference between the security and usability of the authentication method may affect their decision. To make a system usable and secure, system developers need to go beyond the traditional human-centered design techniques and adopt design techniques that allow users to make decisions [5].

Although numerous user studies had examined various authentication methods, such as alphanumeric password [6] [7], graphical password [8][9], and biometrics [10] [11], very limited research investigated users' performance and preference when they were allowed to choose the authentication method(s) for a specific application [12] [13]. We conducted an online empirical study to provide preliminary understanding of the 'Authentication of Choice' (AoC) approach in the context of mobile devices. Authentication of choice is an authentication concept that allows users to select their preferred authentication method(s) out of various methods provided. Three different authentication designs were examined: traditional alphanumeric username and password, one-factor authentication of choice, and two-factor authentication of choice. Preliminary results of the study including the participants' preference over the three authentication designs and the specific authentication methods chosen under the 'authentication of choice' conditions were reported in [14]. This paper presents the performance measures including login time and failed login attempts. More importantly, we present and analyze participants' response to a series of questions that reveals their perception of usability and security in the context of mobile devices as well as how their perception affected their decision when using the 'Authentication of Choice' methods.

The rest of the paper is structured as follows. Section II reviews the literature on authentication methods currently in use and the study related to authentication of choice. We discuss the research methodology for this study in Section III of the paper and the result of the study in Section IV. We addressed the result of the study in Section V of the paper and the conclusion in Section VI.

II. RELATED WORK

There are different authentication methods currently in use. In this section, we review the literature on common authentication methods.

A. Authentication on Mobile Devices

There has been a rapid increase in the use of mobile phones. It was reported in 2016 that almost two-thirds of the world's population has a mobile phone [15]. Mobile devices have improved the quality of life by providing a variety of services anytime and anywhere. However, the mobility and portability of mobile devices pose a significant threat to the privacy and security of the information stored on the device [16]. User authentication is one of the security measures to mitigate the threat to security and privacy of the information on mobile devices. The most popular authentication approach on mobile devices is knowledge-based authentication methods, such as Personal Identification Number (PIN), password, and pattern or graphical passwords. More recently, fingerprint authentication and facial authentication have been widely adopted as well [17].

B. Authentication Methods

There are various authentication methods currently in use. These authentication methods are broadly categorized into four groups based on the factors required for authentication:

I. Knowledge-based Authentication

Knowledge-based authentication uses the information that users must know to verify their identity to the system. Authentication methods in this category require users to be able to recollect some information before gaining access to the system. This is done in form of challenge and response, in which the user responds to the challenge with something he knows [18]. Examples of knowledge-based authentication include numeric password, also referred to as PIN, alphanumeric password, or graphical password. Knowledge-based authentication methods are the most popular form of authentication because they are relatively easy to implement and have lower operating costs [19]. The major limitation of this type of authentication is the memorability requirement. Users have to commit information to memory and recollect the information during the authentication process. This memorability problem does affect the usability and security of knowledge-based authentication methods [18]. Users find it difficult to remember password or PIN and many end up writing down their passwords or choose simple passwords that may result in the compromise of the system security.

II. Inherent factors authentication

Inherent factors authentication, also known as biometrics, uses the physiological or behavioral traits of the user for authentication. These traits include fingerprint, iris, retina, voice, face, signature, typing patterns, physical movement, etc. [20]. To enroll users for biometric authentication, the feature to be used will be captured, processed, and stored in the computer as a baseline to compare with the newly captured biometrics during authentication [21].

Biometric authentication is relatively more usable and secure compared to knowledge-based authentication [22]. One of the challenges of the biometric authentication approach is that once the factor is compromised, the factor will remain compromised forever. There is no way that the user can change his fingerprint like in the case of knowledge-based or possession-based authentication [22]. Another problem with inherent factor authentication is that the user's environment can affect the efficacy of the authentication method [23]. For instance, a health worker in the emergency room wearing gloves and masks may not be able to use fingerprint or face recognition for authentication until they remove their gloves or face mask.

III. Possession-based Authentication

The possession-based authentication, also known as token-based authentication, relies on what users have or possess for authentication. Examples of possession include a token, smart card, common access card, etc. This authentication approach can be used on the stationary computer as a stand-alone device, plug into the computer through the USB port, or installed on a mobile device as an application. The token is widely used in mobile devices. This can be stand-alone hardware or software-based token. The token has a unique cryptographic secret embedded in it that can be used to authenticate using the challenge-response handshake system [24]. If the token device is broken, the key becomes invalid [25]. This authentication approach is relatively more acceptable to users compared to other authentication methods, but it is more difficult to manage, and the device can get lost, stolen or shared [26].

IV. Location-based Authentication

Location-based authentication involves using the geographical location of the user or device to authenticate and validate access to the information system. A common implementation of this approach is when banks deny customer transactions on their debit or credit card in an unauthorized location until the customer calls the bank to provide additional validation. This authentication approach can provide an additional level of security for the system by preventing access from unauthorized areas, but it is not easy to implement and has to be combined with another authentication approach to identify a specific user [27]. Location-based authentication requires a large number of databases and access towers to function effectively [28].

C. Multifactor Authentication Method

Multifactor authentication is a combination of two or more authentication methods to authenticate a user. This was introduced because of the insufficient level of security provided by single-factor authentication [29]. Multifactor authentication provides a higher level of security especially for government and military systems as well as other critical information systems [30]. Combining two or more factors of authentication increases the security of the system, but does affect the usability of the system [31].

D. Authentication of Choice

There is no perfect authentication method that can accommodate the needs of all users [32]. A system designer cannot design a universally accessible authentication method for users without knowing their abilities and disabilities [12]. People have different preferences for authentication methods based on their cognitive skills or physical abilities [13]. Systems are usually designed with one authentication method selected out of a variety of authentication methods that are currently in use. To enhance the security of the system, some systems adopted two-factor authentication that requires a higher workload from the user [32]. In either one-factor or two-factor authentication, providing the freedom of choice in selecting the authentication method(s) preferred by the individual user may improve the usability and the security of the system [14]. To date, there is no known research on the authentication of choice approach. We conducted the following study as an initial attempt to fill in this gap by collecting preliminary data on user performance, preference, and perception of AoC methods on mobile devices.

III. METHODOLOGY

The study was conducted electronically. A within-group design was adopted with three conditions for authentication:

- Alphanumeric username and password
- One-factor AoC: In this condition, participants chose one authentication method out of five options: alphanumeric password, PIN, fingerprint authentication, facial recognition, and One Time Password (OTP).
- Two-factor AoC: In this condition, participants chose two authentication methods out of the five options listed above.

A. Participants

75 participants completed the study. Participants did not receive any financial or other types of incentives for taking part in the study. The participants for the study were selected randomly. The age of participants varies, with 47 participants in the age range of 18-30 years, 18 in the range of 31-40 years, 8 in the range of 41-50 years and 2 above 50. Out of the 75 participants, 43 claimed they were male while 32 claimed to be female. 71 of the participants were professionals working in various fields, such as business, education, science, engineering and IT, and healthcare. Three participants were students. One participant did not identify his/her career. Regarding educational background, 31 participants claimed to have a high school diploma, 33 participants had bachelor degree and 11 participants had postgraduate degrees. The level of information security experience of the participants varies: 28 participants claimed themselves as experts, 23 with intermediate knowledge, and 23 with basic level of experience. One participant did not respond to this question.

B. Event Manager Application

An Android-based mobile device application called 'Event Manager' was developed to provide a realistic setting for this study. The 'Event Manager' supports five authentication methods and provides a calendar for managing daily schedule. The calendar function was chosen because it was available on almost all mobile phones and its' security and privacy related expectation was representative of many tasks conducted on mobile devices on a daily basis. The five authentication methods supported are commonly adopted on mobile devices:

- Alphanumeric username and password
- PIN
- Fingerprint authentication
- Facial recognition
- One-Time-Password (OTP)

The design of the application followed general usability guidelines and underwent several rounds of refinement based on users' feedback. The home page and the registration page of the application are demonstrated in Figure 1 (a and b). Users can create three types of accounts on the application using the same email:

Type 1 (T1): Alphanumeric username and password
Type 2 (T2): One-factor AoC out of five options
Type 3 (T3): Two-factor AoC out of five options

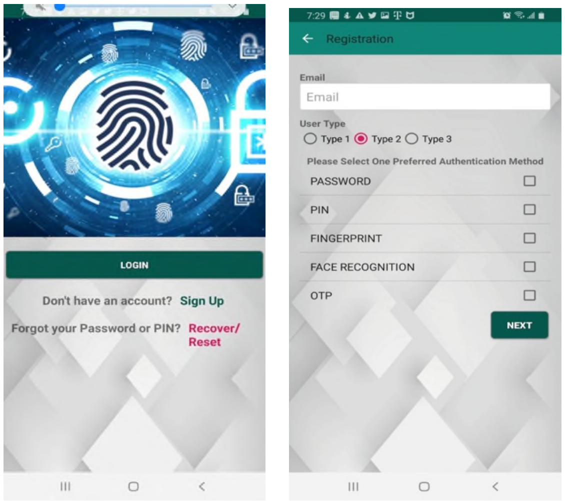
LOGIN
Don't have an account? Sign Up
Forgot your Password or PIN? Recover/ Reset
7:29
Registration
Email
Email
User Type
○ Type 1 ● Type 2 ○ Type 3
Please Select One Preferred Authentication Method
PASSWORD □
PIN □
FINGERPRINT □
FACE RECOGNITION □
OTP □
NEXT

Figure 1. (a) Home page and (b) Registration page.

C. Procedure

This study was conducted electronically. Instructions for the study and the questionnaire link were sent out to participants via email. After providing consent to take part in the study, participants first downloaded the 'Event Manager' app from Google Play and installed it on their Android phones. Then, each participant created and logged into an account under all three conditions. After they logged into an account, they added or revised an event on the calendar. The order of the three conditions was counterbalanced among the participants to control the learning effect. After the participants completed the tasks under all 3 conditions, they answered a questionnaire via a Google Form. The questionnaire collected participants' demographic information, their general attitude toward security and privacy, their security-related practice on their mobile devices, and their preference and perception towards the AoC approach. The authentication methods chosen during the two AoC conditions, the time it took to login, and the outcome of the login attempt were automatically logged by the application.

IV. RESULTS

In this section, we discuss the result of the study using the data obtained from the Event Manager application and the questionnaire completed by participants.

A. Login time and failed attempts

A One-Way Repeated Measures ANOVA test using login time as the dependent variable and condition as the independent variable suggests that there is significant difference in the login time under the three conditions (F (2, 148) = 56.80, $p < 0.001$). Post hoc Least Significant Difference (LSD) tests suggest that the participants took significantly longer time to login under the alphanumeric username/password condition than the one-factor AoC condition ($p < 0.001$) and the two-factor AoC condition ($p < 0.05$). Participants also took significantly longer time to login under the two-factor AoC condition than the one-factor condition ($p < 0.001$).

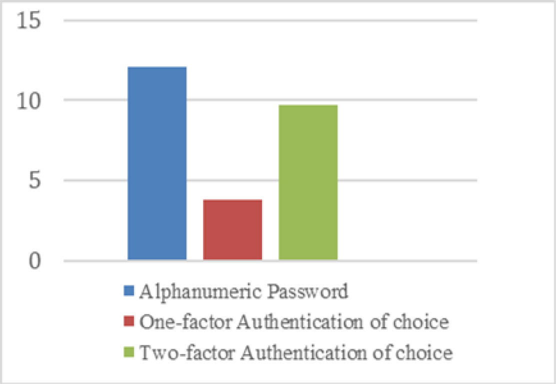

Figure 2. Login time for the three authentication conditions.

Failed login attempts rarely occurred during the study. There were five instances of incorrect alphanumeric password, two instances of unrecognized fingerprint, and two instances of unrecognized face.

B. Attitude toward security and usability

Participants were asked to rate the importance of security and privacy of their information; 67 (89%) participants claimed that it was very important, 5 (7%) claimed it as fairly important while 3 (4%) claimed it as important. When asked about the importance of security of their mobile phone, 69 (92%) participants rated it as very important, 4 (5%) as fairly important, 1 (1%) as important while the remaining 1 (1%) as slightly important.

Participants rated the level of importance regarding the security and ease of use of the authentication method on their mobile phone. Table I illustrates the number of participants that ranked the importance of security and ease of use at a specific level. Out of 75 participants, 69 (92%) believed security is very important and the remaining 6 (8%) claimed that is it fairly important. 63 (84%) participants claimed ease of use is very important, 6 (8%) participants claimed it as fairly important and the remaining 6 (8%) claimed it as important.

TABLE I. PARTICIPANTS RANKING OF SECURITY AND EASE OF USE

Level of Importance	Security	Ease of use
1 (Not at all)	0	0
2 (Slightly important)	0	0
3 (Important)	0	6
4 (Fairly important)	6	6
5 (Very important)	69	63

Participants were asked whether they would choose ease of use over security regarding mobile phone authentication. Out of 75 participants, 47 strongly disagreed, 10 disagreed, 5 were neutral, 7 agreed and 4 strongly agreed.

C. Current practice regarding mobile phone authentication

67 (89%) participants normally secured their phone while 8 (11%) did not. Table II illustrates the number and percentage of participants that used a specific authentication method to secure their phones.

TABLE II. PARTICIPANT AUTHENTICATION METHOD PREFERENCE

Authentication method	# of participants	# of participants
Alphanumeric password	27	36%
PIN/ Passcode	67	89%
Gesture /Pattern	40	53%
Fingerprint	59	79%
Facial authentication	48	64%

D. User perception of authentication on mobile phones

Based on their perception, participants selected an authentication method that they believed was the most secure and one they believed was the easiest to use on mobile phones. Table III illustrates the number of participants that rated the two elements at a specific level.

TABLE III. AOC BASED ON SECURITY AND EASY OF USE

Methods	Most Secure	Easiest of use
Alphanumeric password	2	2
PIN	2	6
Fingerprint	50	42
Facial authentication	18	23
Gesture/Pattern	1	2
Voice authentication	2	0

As illustrated in Table IV, the majority of the participants chose fingerprint as the most secure (67%) and the easiest to use (56%) authentication method. The second on the list is facial authentication, with 18 participants choosing it as the most secure and 23 participants as the easiest to use. All the other methods received much fewer votes on both perspectives. No participant chose OTP to be the most secure or easiest to use.

Participants were asked to rank four criteria for selecting an authentication method on a mobile phone, namely efficiency, ease of use, security, and memorability. Table IV illustrates how participants ranked the four criteria. Security was chosen to be the top rank criteria when selecting an authentication method by 56 (75%) participants, followed by the ease of use, efficiency, and memorability.

TABLE IV. CRITERION RANKING

Rank	**Efficiency (quick)**	**Ease of use**	**Security**	**Memorability**
Top rank	8	11	56	0
2nd rank	20	28	16	11
3rd rank	31	26	3	15
4td rank	16	10	0	49

Participants ranked their preference towards the three authentication conditions. The results were reported in [6]. Participants overwhelmingly preferred the one-factor AoC condition over the other two conditions. 63 participants chose the one-factor AoC as their top choice while 9 selected the two-factor AoC and 3 selected the alphanumeric password method. To further understand their preference, we asked participants to select the possible reasons behind their ranking. Four possible reasons were provided: efficiency, ease of use, security, and memorability. Participants could check multiple reasons that applied. Table V illustrates the number of participants that selected each condition as their top preference and the number of participants in that group who selected each specific reason.

TABLE V. TEST CONDITIONS CHOICE BASED ON CRITERION

	Alphanumeric password as top preference	**One-factor AoC as top preference**	**Two-factor AoC as top preference**
Number of participants	3	63	9
Efficiency	2	34	3
Ease of use	2	51	3
Security	2	54	7
Memorability	0	28	1

Among the 63 participants who chose one-factor AoC as their top preference, 54 participants selected security and 51 selected ease of use as one of the reasons for their decision, suggesting that the two factors are the dominant factors in the decision making process regarding the selection of authentication approach on mobile phones.

Finally, we asked participants whether two-factor AoC improves the security of the system, requires too much time for authentication, is difficult to remember, or difficult to use. We asked these questions to evaluate their perception of the two-factor AoC approach.

TABLE VI. PERCEPTIONS OF TWO-FACTOR AOC

Perceptions	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
Improves Security	0	2	5	11	56
Takes too much time	17	25	11	13	8
Difficult to remember	29	29	11	5	0
Difficult to use	21	34	11	7	1

Among the 74 participants who answered these questions, 67 agreed that using two-factor AoC improved the security of the authentication process. When asked whether two-factor AoC took too much time, 42 participants disagreed, 11 were neutral and 21 agreed. 58 participants disagreed that the two-factor AoC was difficult to remember, 5 agreed and 11 were neutral. 55 participants disagreed that using two-factor AoC made the authentication process difficult, 8 agreed and 11 were neutral.

V. DISCUSSION

The results suggested that, on a mobile phone, both the one-factor authentication and the two-factor authentication are significantly more efficient than the alphanumeric password method. The participants highly valued security and privacy both from the general perspective and in the specific context of mobile phone usage.

The study revealed an interesting contradiction between users' perception about security and their actual security decision. 92% of participants rated security as very important in general and 75% chose security as their most important criteria when selecting an authentication method for their mobile phone. However, 84% of the participants prefer one-factor AoC over two-factor AoC even though 89% of them agreed that two-factor AoC could improve the security of the device. This finding suggests that users should not be expected to choose the most secure authentication method available even though they highly value security. The reason could be attributed to the classic tradeoff between security and usability. In this study, 51 out of the 63 participants who chose one-factor AoC as their top preference selected 'ease of use' as one of the reasons for their decision. So, between one-factor and two-factor authentication, it seems that most users would prefer the one-factor AoC due to its efficiency and reduced cognitive load.

One-factor AoC may not support the level of security protection desired or required by many institutions, businesses, or individual users. In those cases, is it feasible to require two-factor AoC? The finding of the study provides a positive answer to that question. Although the participants overwhelmingly preferred one-factor AoC over two-factor

AoC, their perception about two-factor AoC is highly positive. 89% of the participants thought two-factor AoC could improve security. 71% and 92% of the participants were fine with the efficiency and memorability of two-factor AoC, respectively. 87% thought the general usability of the two-factor AoC was acceptable. Therefore, when one-factor AoC is not an option, it is quite likely that users would adopt two-factor AoC and find it usable.

As a preliminary investigation of the authentication of choice approach, this study has several limitations that need to be addressed through future research. First, the study only involved Android users and the results may not be generalizable to users of other platforms. Second, the authentication methods supported were either knowledge-based or biometrics. Possession-based and location-based authentication methods were not examined. Third, because the participants logged into each account only once during the study, the result only applies to the very initial interaction with the different authentication options. We are planning a one-month longitudinal study to examine the AoC approach in a more realistic setting.

VI. CONCLUSION

This study provided insights about user performance, preferences, and perception of the authentication of choice approach on mobile devices during their initial interaction with this approach. The efficiency and the user subjective perception suggest that the AoC approach has the potential to serve as a usable and secure authentication solution on mobile devices. Although users overwhelmingly prefer the one-factor AoC over two-factor AoC, they are likely to adopt the two-factor AoC when a higher level of security protection is desired or required. Future research is needed to confirm the findings of this study on other platforms and longer period of user interaction.

VII. ACKNOWLEDGMENT

We sincerely appreciate Edward Miklewski for his assistance in data collection and our appreciation goes to all the participants of this study.

VIII. REFERENCES

[1] E. Davidson, B. McCredie, and W. Vikelis, IBM Dictionary of Computing. Edited by G. McDaniel. 10th ed. New York, NY: McGraw-Hill, 1994.

[2] R. Clarke, Sufficiently Rich Model of (id)Entity, Authentication and Authorization

http://www.rogerclarke.com/ID/IdModel1002.html#MAc, [retrieved: November, 2020].

[3] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behavior in organizations," In Proceedings of the workshop on new security paradigms, pp. 47-58, 2010. doi: 0.1145/1595676.1595684.

[4] K. P. Yee, User Interaction Design for Secure Systems. In Proceedings of the 4th International Conference on Information and Communications Security, Singapore, pp. 278-290, 2002.

[5] L. F. Cranor and N. Buchler, "Better Together: Usability and Security Go Hand in Hand," in IEEE Security & Privacy, vol. 12, no. 6, pp. 89-93, 2014. doi:10.1109/MSP.2014.109

[6] R. Anderson, J. Yan, A. Blackwell, and A. Grant, Password memorability and security: Empirical results. IEEE Security and Privacy, 2(5), pp. 25–30, 2005.

[7] J. Yan, N. H. Zakaria, D. Grifths, and S. Brostof, Shoulder surfing defense for recall-based graphical passwords. In: Proceedings of the seventh symposium on usable privacy and security (pp 6:1– 6:12), 2011. New York, NY, USA: ACM. https://doi.org/10.1145/20788 27.2078835, [retrieved: November, 2020].

[8] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, pp. 45-58 , 2000.

[9] A. M. Eljetlawi and N. Ithnin, Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods. Convergence and Hybrid Information Technology, pp. 1137-1143, 2008.

[10] A. H Mir, S. Rubab, and Z.A Jhat, Biometrics Verification: a Literature Survey. Journal of Computing and ICT Research, Vol. 5, Issue 2, pp. 67-80, 2011.

[11] S. Cohen, N. Ben-Asher, and J. Meyer, Towards information technology security for universal access. In: Stephanidis, C. (ed.) Universal Access in HCI, Part I, HCII 2011. LNCS, vol. 6765, pp. 443–451. Springer, Heidelberg.

[12] P. Fairweather, V. Hanson, S. Detweiler, and R. Schwerdtfeger, From assistive technology to a web accessibility service. In Proceedings of the 5th International ACM Conference on Assistive Technologies (ASSETS). ACM, pp. 4-8, 2002.

[13] M. Belk, C. Fidas, P. Germanakos, and G. Samaras, Security for diversity: Studying the effects of verbal and imagery processes on user authentication mechanisms. In IFIP TC13 Conference on Human-Computer Interaction (INTERACT). Springer, pp. 442-459, 2013.

[14] A. J. Oluwafemi and H. D. Feng, Authentication of Choice on Mobile Devices: A Preliminary Investigation. Human-Computer Interaction international conference 2020, in press.

[15] S. Kemp, Digitalin 2017: Global Overview.' We Are Social, 2017, https://wearesocial.com/specialreports/digital-in-2017-global-overview [retrieved: November, 2020].

[16] R. Marcin, S. Khalid, R. Mariusz, T. Marek, and A. Marcin, User Authentication for Mobile Devices. 12th International Conference on Information Systems and Industrial Management (CISIM), Sep 2013, Krakow, Poland. pp.47-58, ff10.1007/978-3-642-40925-7_5ff. ffhal01496111

[17] P. S. Teh, N. Zhang, and S. Tan, Strengthen user authentication on mobile devices by using user's touch dynamics pattern. J Ambient Intell Human Comput, pp 4019-4039, 2020 https://doi.org/10.1007/s12652-019-01654-y,[retrieved: November, 2020].

[18] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, Security and Usability in Knowledge-based User Authentication: A Review, 2016. 10.1145/3003733.3003764.

[19] B. W. Lampson, Computer Security in the Real World, IEEE Computer, vol. 37, no. 6, pp. 37 - 46 , 2004. ISO 9564-1:2011

[20] S. C. Fang and H. L. Chan, Human identification by quantifying similarity and dissimilarity in electrocardiogram phase space. Pattern Recogn. 42, pp. 1824–1831, 2009. https://doi.org/10.1016/j.patcog.2008.11.020, [retrieved: November, 2020].

[21] F. L. Podio and J. S. Dunn, Biometric Authentication Technology: from the Movies to Your Desktop, ITL Bulletin , 2001.

[22] C. Stephanidis and M. Antona, UAHCI/HCII 2013, Part I, LNCS 8009, pp. 195–204, 2013. Springer-Verlag Berlin Heidelberg

[23] D. Bordea, Selecting a two-factor authentication system. Network Security, p. 17-20, 2007.

[24] R. Sandhu and P. Samarati, Authentication, access control, and audit. Computing Surveys (CSUR), Vol. 28, 1, pp. 241-243, 1996.

[25] A. Habtamu, Different Ways to Authenticate Users with the Pros and Cons of each Method, Norwegian: Norsk Regnesentral, pp. 350-364, 2006.

[26] R. Sailer, X. Zhang, T. Jaeger, and L. Van Doorn, "Design and Implementation of a TCGbased Integrity Measurement Architecture", Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, SSYM'04, USENIX Association, Berkeley, CA, USA, pp. 16–16, 2004

[27] S. Holtmanns, V. Niemi, P. Ginzboorg, P. Laitinen, and N. Asokan, Cellular Authentication For Mobile And Internet Services, Wiley, UK, 2012.

[28] R. K Konoth, V. Van der Veen, and H. Bos, How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, pp. 405–421, 2016.

[29] R. K Banyal, P. Jain, and V. K. Jain, Multi-factor authentication framework for cloud computing. In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, Korea, pp. 105–110, 2013.

[30] E. De Cristofaro, H. Du, J. Freudiger,, and G. Norcie, A comparative usability study of two-factor authentication. arXiv preprint arXiv:1309.5344, 2013.

[31] K. Renaud, Quantification of authentication mechanisms - a usability perspective. Journal of Web Engineering, 3(2), pp. 95-123, 2004.

[32] A. Jain, A. Ross, and K. Nandakumar, Introduction to biometrics. Springer 2011 edition, pp. 947-954, 2011.