KidsDoodlePass: An Exploratory Study of an Authentication Mechanism for Young Children

Esra Alkhamis, Helen Petrie, Karen Renaud

KidsDoodlePass: an Exploratory Study of an Authentication Mechanism for Young Children

Esra Alkhamis[1,2][0000-0002-0019-0241], Helen Petrie[1][0000-0002-0100-9846] and

Karen Renaud[3][0000-0002-7187-6531]

[1] Department of Computer Science, University of York, York, United Kingdom
[2] Department of Information Technology, King Saud University, Riyadh, Kingdom of Saudi Arabia
[3] School of Design and Informatics, Abertay University, United Kingdom
ea921@york.ac.uk, helen.petrie@york.ac.uk, k.renaud@abertay.ac.uk

Abstract. Textual passwords are problematic for young children, whose cognitive, memory and linguistic capabilities are still developing. A possible alternative to using text for authentication systems for young children is drawings. In this paper, we describe an authentication system called KidsDoodlePass, which use simple drawings ("doodles") that the children themselves create. An initial evaluation of the system was undertaken with 19 children aged 6 to 9 years of age. Success of logging in with KidsDoodlePass was high, only on few occasions did a child need more than one attempt, demonstrating that the system is effective. Selection times dropped significantly on the second use of the KidsPassDoodle and were typically under 10 seconds per grid. Most children thought their KidsDoodlePass would be easier to remember than a text password, a significant proportion. These positive results suggest that KidsDoodlePass could be a useful mechanism for young children to use as a first experience of authentication and a useful first step toward adult authentication systems.

Keywords: Authentication systems, usable security, KidsDoodlePass, children.

1 Introduction

Young children increasingly use electronic devices and the Internet and therefore may need to use passwords to access their devices or online accounts. UNICEF estimates that worldwide for every three adult Internet users, there is one child user [27]. In the USA, it was estimated that in 2015 60% of children aged 3 to 17 years used the Internet at home [3]. This number had increased nearly six-fold since 1997, when it was only 11%. In the UK, more than half of all children now use the Internet [21]. This means that children are probably using passwords when their cognitive, memory and linguistic capabilities are still developing, and they may not have the appropriate capability to create and remember appropriately strong passwords, nor understand the importance of password best practices.

As young children's vocabulary and spelling skills are still developing, if they are asked to create their own passwords they tend to be short, simple words within the

scope of their vocabulary and they may misspell passwords when trying to remember them [4, 5, 22]. In terms of cognitive development, young children are at the egocentric stage of development [13], so will be likely to create passwords which are related to themselves [17, 18] and which therefore may be very easy to break. More specifically, in terms of cognitive development, young children are in process of developing "theory of mind" or meta-cognitive processes [9, 10]. This concept refers to understanding what other people will know and understand. For example, if a child shares their password with a parent, but they are then asked to change it, until they develop a theory of mind, they will assume that the parent knows the new password. Finally, another specific aspect of cognitive development relevant to password creation and use is semantic memory and metamemory [11]. A password is a specific piece of information which needs to be remembered; children must understand the need to remember this information and have strategies for remembering it which will help them retrieve the information when it is required. Young children will not yet have developed all these skills.

A problem with asking children to undertake password practices which are beyond their linguistic and cognitive abilities is that they may teach young children poor password practices which then endure as they grow up. Graphical passwords are worth exploring as possible alternatives to text passwords for children, to begin to teach them about the importance of authentication, but using procedures which are within their skill set. There are several benefits of this alternative: using graphical information created by the child themselves is within the realm of self-related information appropriate for the egocentric stage of development; graphic information also overcomes issues of the child's stage of linguistic development, both for creation and later spelling of passwords; finally, in relation to memory development it relies on recognition rather than recall, which is cognitively far less demanding.

In this paper, we present a graphical authentication system designed specifically for young children, which is built on doodles (simple drawings) the children create themselves. We present an initial evaluation with children aged 6 to 9 years, assessing effectiveness, efficiency and satisfaction of the system.

2 Related Research

A number of studies have investigated children's understanding and use of text passwords. Read and Cassidy [22] found that 7 to 8 year old children had a basic understanding of password principles: they should be hard to guess, but simple to remember; and they should prevent other people accessing the children's devices. These researchers also asked children 6 to 10 years old to create a password. All the children created simple passwords, with younger children creating even simpler ones than older children. The children often created passwords which were easily guessable from their username and 13% misspelled their password when they came to use it. In a follow-up study, Lamichhane and Read [17] found that over half a sample of 7 to 8 year old children created self-related passwords. Coggins [2] investigated similar issues with children aged 9 to 11 years. The children in his study had some idea of how to

create good passwords, as they used at least six characters and a combination of letters and digits. But only 27% of the passwords created were assessed as being "strong".

Many graphical password authentication systems have been proposed for adults, starting with the Draw-a-Secret (DAS) system proposed by Jermyn et al. [16, see 1 for a review]. Many of these systems are based on the recognition of pictures, either of human faces [6, 8] or objects [7], but some involve user-generated drawings in different ways [12, 15, 25, 27], including a system specifically for older users [23]. Some research has investigated graphical systems specifically for children. Several studies conducted in Japan investigated graphical authentication for primary school children [19, 20]. These studies used icons such as animals, flowers, and fruit. The components of the password could be remembered easily, but the children often chose them in the wrong order. Renaud [24] developed am authentication mechanism specifically for children using images the children drew called Mikons ("my icons"). Children aged 11 to 12 years were able to identify their own Mikons with ease. After three months the children had no difficulty remembering their Mikon passwords, despite the long delay. Imran [14] compared three graphical authentication mechanisms (PassTiles) using different image types: objects, images and words. These were tested with both adults and children aged 7 to 12 years. The children performed best with object PassTiles in which they recognised images of distinct objects from decoys. The word PassTiles were more difficult for children to recall. Adults and children both demonstrated a preference for graphical passwords over existing text passwords mechanisms.

Although there has been a great deal of research carried out in the graphical authentication area for adults, there has been little research on this topic for children for whom this kind of authentication system might be a useful first step to learning about authentication systems and their importance.

3 Method

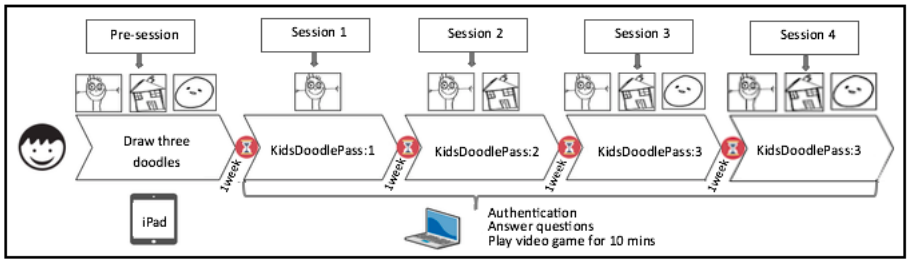

Fig. 1. Design of the Study.

The design in the study is summarized in Fig. 1. Children aged 6 to 9 were asked to use the "KidsDoodlePass" authentication system. Instead of being a textual password, their KidsDoodlePass consisted of one, two or three doodles (i.e. simple drawings), which they drew at the beginning of the study. The authentication mechanism tested their ability to correctly identify their own doodle displayed in a series of 3 x 3 grids with a range of distractor doodles (see Fig. 2). Each grid included another doodle from the three they had created themselves, a doodle in the same category created by another

child and six other randomly selected doodles from other children participating in the study.

The study involved a pre-session and four experimental sessions, each approximately one week apart (see Fig. 1). At the pre-session, the children created three doodles. At the first experimental session, they chose one of their doodles for their KidsDoodlePass:1. They then used it to log in to an online games area. If they failed to recognize their KidsDoodlePass:1 three times, they were given a hint by the researcher. If that failed, the researcher identified their KidsDoodlePass:1 doodle (this protocol of attempts, hints and assistance was followed for all logins). The children then played an age-appropriate game for 10 minutes, which acted as both a reward and a distractor task to allow investigation of whether they remembered the KidsDoodlePass:1 after a short time. After the play period, they were asked to log in again with KidsDoodlePass:1.

At the second session, children logged in with KidsDoodlePass:1, played a game and then logged in again with KidsDoodlePass:1. They then chose a second doodle to create their KidsDoodlePass:2 (they were told this would make their KidsDoodlePass stronger) and then logged in with that. The KidsDoodlePass:2 authentication process required them to traverse two grids of nine doodles each, correctly identifying their doodle each time.

At the third session, the procedure from the previous sessions was repeated. This time, the children started with their KidsDoodlePass:2, played a game, logged in again with KidsDoodlePass:2, then created KidsDoodlePass:3, consisting of all three doodles they had drawn. The KidsDoodlePass:3 authentication process involved traversing three grids of nine doodles each. At the fourth session, the children logged in with KidsDoodlePass:3, played a game and logged in again with KidsDoodlePass:3.

During each session, children were asked a number of questions about their use of computing devices, and their knowledge and use of passwords and authentication mechanisms.

Thus, a repeated measures design was used, with one within-participants independent variable, the number of doodles in the KidsDoodlePass. The dependent variables were: (1) the accuracy of remembering the KidsDoodlePass, to measure effectiveness and (2) the time taken to select their doodles, to measure efficiency. Satisfaction was measured by the questions asked during the sessions.

3.1 Participants

19 children took part, all were recruited from a private international school in Riyadh, Saudi Arabia. 10 boys and 9 girls. 6 were in Grade 1 (6 - 7 years old), 6 in Grade 2 (7 - 8) and 7 in Grade 3 (8 - 9). All children had some experience with passwords and authentication systems, either for accessing devices or online accounts. The children used a range of electronic devices, the most popular being tablet computers, used by 13 (68.4%) of the children, followed by smartphones (57.9%), game consoles (36.8%) and desktop/laptop computers (26.3%). 18 of the 19 children (94.7%) had used passwords. 8 children (42.1%) had used them for devices only, a further 8 (42.1%) used them for devices and online accounts and one child (5.3%) used them for online accounts only.

The children were offered a gift voucher worth the equivalent of USD 13 to spend at a local bookstore for participating in the study.

Fig. 2. Authentication grid of nine doodles for KidsDoodlePass.

3.2 Study Website and equipment

A website was developed to present the KidsDoodlePass authentication system, to give children access to a range of age-appropriate video games and to collect data about the accuracy and timing of their responses to the KidsDoodlePass system.

The website was developed using PHP, JavaScript and XML with a MySQL database. The website consists of a username page in which the researcher enters the child's participant code, so session information is correctly stored. There is then one, two or three pages for authentication, depending on which KidsDoodlePass is being used at the time. When a doodle is selected, it is highlighted by a box, (see Fig. 2), so the child can change their mind about their selection before attempting to log in. The authentication pages are programmed to record the number of attempts the child makes to log in, whether they are correct or not and how long the child spends on each page from when the page appears to when the child hits the login button.

The children drew their doodles on a 9.7 inch Apple iPad (6th Generation), running iOS 11.2.6, using a MPIO Stylus Pen with a 1.5mm tip. The experimental sessions were all run on a 13 inch MacBook Air running MacOS High Sierra (version 10.13.4), with a 1.8 GHz Intel processor. The games used were selected from the PBS Kids website (pbskids.org).

3.3 Procedure

The study was approved by the Physical Sciences Ethics Committee of the University of York. Permission was then sought from the Head of Al Forsan International School in Riyadh who sent letters to parents of children in Grades 1 to 3. Parents replied to the

Head with a physical letter of consent if they were happy for their child to participate in the study. The school gave permission for the children to take part in the study during their weekly art classes. The first author gathered all the data. She was given a quiet room at the school to meet the children and conduct the study.

At the beginning of the pre-session the children's consent to participate in the research was sought. They were asked if they would help the researcher with her work which would involve creating logging into an online account a number of times. If they did so they would be able to play video games and receive a gift voucher. They were then asked to draw three simple doodles on the iPad. They were told to draw three simple objects and that there was no need to make a perfect drawing. After each drawing, the children were asked what the doodle represented.

The doodles were categorized before the first experimental session to allow creation of KidsPassDoodle grids with appropriate combinations of doodles. Categorisation of the doodles started with the children's own descriptions and was then refined by the first author. In some cases, doodles were grouped differently if they seemed similar to other children's doodles and could easily belong to the same category. In total, 23 different categories were created.

At the beginning of each experimental session, the child was told that they could play an online game but, in order to keep the game private, they needed to have an account and that their doodles would be used as their password. At the beginning of the first session, they were asked to select one of their three doodles as their KidsDoodlePass. They were then asked to log in to the games area. If they could not identify their doodle from the 3 x 3 grid, or chose an incorrect doodle, a friendly error message appeared: "*Oops! Something went wrong. Please try again*". The child had three attempts at identifying their doodle, after which the researcher gave them a hint (e.g. if the doodle was a flower, the child was told the correct doodle was something natural). If the child could still not identify their KidsDoodlePass, the researcher showed them the correct one with reassurance: "*It's OK, I will help you, but you need to try to remember it for next time*".

When the child successfully logged in, there was a selection of games to play. They played for 10 minutes, after which the researcher asked them to log in again (they were told this was to check the game) and they were told: "*Now we need to make your KidsDoodlePass stronger so we will choose a new doodle*." In sessions 2 and 3 they were then taken to the page to choose another doodle to add to their KidsDoodlePass, and asked to log in again with the new KidsDoodlePass to test it out. They were then thanked for their participation and told there would be another session in about a week's time, if appropriate. At the end of session 4 they were thanked for their participation in the study, asked whether they had any questions about the study and given their gift voucher.

4 Results

Table 2 summarizes children's accuracy in selecting the correct doodles on each grid, the measure of the effectiveness of the authentication system. Children were in general

very accurate in selecting the doodles, even on the three doodle KidsDoodlePass:3. On only a small number of occasions did children need a second attempt. Only one child needed a third attempt to recognise their doodle and only on two occasions did a child need a hint. In both the latter instances, the child repeatedly selected the same incorrect doodle from their own doodles. In addition, there was only a small drop in accuracy with increasing complexity of KidsDoodlePass, with KidsDoodlePass:3 showing slightly lower accuracy rates than KidsDoodlePass:2.

The selection times were not normally distributed (as is typical of reaction times), so medians were used to summarize the data and non-parametric statistics conducted. Fig. 3 presents the median times to select the correct doodle. For KidsDoodlePass:1, there was a significant decrease in the selection time from the first to the second login (before and after playing the game) (Wilcoxon Signed Rank Test = 24.0, p = .013). None of the other differences between the selection times for the individual grids were significant.

Table 1. Summary of KidsDoodlePass accuracy (Percentage of children who correctly select each doodle at first attempt, for each grid of doodles).

KidsPass Doodle	Session 1	Session 2	Session 3	Session 4
1	Login 1: 100.0 Login 2: 89.5	Login 1: 94.7 Login 2: 84.2		
2		Login 1: Grid 1: 94.7 Grid 2: 100.0	Login 1: Grid 1: 94.7 Grid 2: 100.0 Login 2: Grid 1: 94.7 Grid 2: 94.7	
3			Login 1: Grid 1: 100.0 Grid 2: 100.0 Grid 3: 94.7	Login 1: Grid 1: 94.7 Grid 2: 100.0 Grid 3: 94.7 Login 2: Grid 1: 94.7 Grid 2: 89.5 Grid 2: 94.7

In terms of satisfaction with the system in comparison to text passwords, when asked which system they preferred 12 (63.1%) children said they preferred KidsDoodlePass and 6 (31.5%) said they preferred text passwords, but this difference was not significant. (chi-square = 2, df = 2, n.s.). At the end of Session 4, after using KidsDoodlePass:2 and KidsDoodlePass:3 three times each, the children were asked whether they thought remembering the KidsDoodlePass:3 was harder than the KidsDoodlePass:2. 17 (89.4%) children thought they were equal in difficulty, the other 2 (10.5%) thought remembering KidsDoodlePass:3 was harder, a significant difference (chi-square = 11.84, df = 1, p = .0005). The children were also asked whether they thought they would be able to remember three doodles as a KidsDoodlePass for a long time. 11 children (57.8%) answered positively, 4 (21.1%) said they would not remember and 4 (21.1%) were not sure, not a significance difference (chi-square = 5.16, df = 2, n.s.).

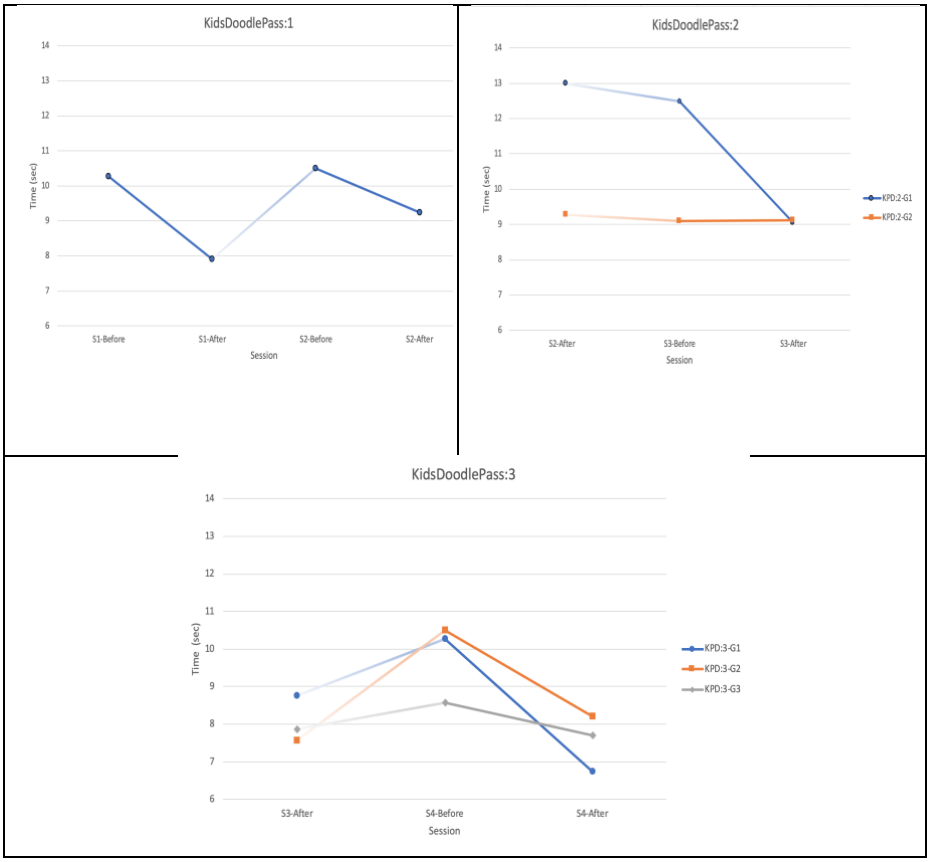

Fig 3. Time (seconds) to select each doodle for each KidsDoodlePass grid of doodles (shaded lines show transitions between sessions, one week apart)

5 Discussion and Conclusions

Our study was an initial investigation of the effectiveness, efficiency and satisfaction of a doodle-based authentication system, KidsDoodlePass, for young children aged 6 to 9 years. In terms of effectiveness, the system worked very well, the all children successfully logged in 10 times, only once was a hint required and the researcher never had to log in for a child. In terms of efficiency, children only needed less than 10 seconds on average for each grid with a certain amount of practice. So, logins, even with three doodles would take less than 30 seconds, which seems very acceptable. Further research is needed to compare efficiency to traditional text passwords for children in this age group. This was not attempted in the present study, as we were

unsure whether the doodle-based system would be effective. However, compared to Read and Cassidy's [22] results on children's ability to recall a text password, the KidsDoodlePass system is very effective. In their study, of the younger children (6 to 7 years), 23.1% failed to recall a password they had created themselves after an hour, whereas all our children recognised their KidsDoodlePass even after a week. However, this is in contrast to the results of Cole, Walsh and Pease [5] who compared performance with self-generated graphical and text passwords by children aged 6 to 12 years. The found that children had higher success rates with text passwords than with graphical passwords, both after a distraction task and two weeks later. Order of password elements was one of the difficulties children encountered, which was only a minor problem in our study. In terms of satisfaction, a significant proportion of children said the doodles for KidsDoodlePass were easier to remember than regular passwords. However, only 12 out of the 19 children said they preferred KidsDoodlePass to a text password, which was not a significant proportion, but a reasonable proportion given the small sample size

Several limitations and issues with the study need to be noted. This was a small scale evaluation with only 19 children to make an initial assessment of the effectiveness, efficiency and satisfaction of the KidsDoodlePass authentication system. Given this initial success, a larger evaluation with more children, and a comparison with passwords, is planned. In retrospect, a particular child should only ever see one of their own doodles in a grid. This design improvement might help reduce the ordering confusion, although this was only a minor problem.

We evaluated KidsDoodlePass, a graphical alternative to text password authentication for young children. We found that they were largely able to identify their own doodles appropriately, and could log in successfully using the system. Due to this successful initial experience of the children while using KidsDoodlePass, we are planning to refine the system and evaluate it with a larger group of children, extending the age range to 6 to 12 years. In addition, we will evaluate longer term memorability of KidsDoodlePass by investigating its use over a period of a month.

References

1. Biddle, R. Chiasson, S. & van Oorschot, P.C. (2012). Graphical passwords: learning from the first twelve years. *ACM Computing Surveys*, 44(4), Article 19.
2. Coggins, P.E. (2013). Implications of what children know about computer passwords. *Computers in the Schools*, 30 (3), pp 282-293.
3. ChildTrends (2018). Home computer access and Internet use. Available at: https://www.childtrends.org/indicators/home-computer-access (Accessed: 7 January, 2020).
4. Choong, Y.-Y. Theofanos, M., Renaud, K. & Prior,S. (2019). Case study – exploring children's password knowledge and practices. In *Workshop on Usable Security (USEC)* 2019. San Diego, CA.
5. Cole, J. Walsh, G. & Pease, Z. (2017). Click to enter: Comparing graphical and textual passwords for children. In *2017 Conference on Interaction Design and Children (IDC '17*). ACM, New York, NY, USA, 472–477.
6. Davis, D. Monrose, F. & Reiter, M. (2004). On user choice in graphical password schemes. In *13th USENIX Security Symposium*.

7. Dhamija, R. & Perrig, A. (2000). Deja Vu: A user study using images for authentication. In *9th USENIX Security Symposium.*
8. Dunphy, P. Nicholson, J. and Olivier, P. (2008). Securing Passfaces for description. In *4th ACM Symposium on Usable Privacy and Security (SOUPS).*
9. Flavell, J. (1999). Cognitive development: children's knowledge about the mind. *Annual Review of Psychology*, 50, 21 – 45.
10. Frith, C. and Frith, U. (2005). Theory of mind. *Current Biology*, 15(17), pp. R644-R646
11. Gathercole, S. (1998). The development of memory. *Journal of Child Psychology and Psychiatry*, 29(1), 3 – 27.
12. Goldberg, J., Hagman, J. Sazawal, V. (2002). Doodling our way to better authentication. *Extended Abstracts on Human Factors in Computer Systems (CHI EA '02).*
13. Hurlock, E.B. (2017). *Child development*, 6th edition. McGraw Hill.
14. Imran, A. (2015). *A comparison of password authentication between children and adults*. PhD dissertation. Carleton University, Canada.
15. Jebriel, S.M., Alali, H & Abuzaraida, M.A. (2015). Investigating the usability of using Doodle Scan System (DSS): The case of Misurata. In *IEEE International Conference on Service Operations and Logistics and Informa*tics (SOLI). IEEE.
16. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. & Rubin, A. (1999). The design and analysis of graphical passwords. In *8th USENIX Security Symposium.*
17. Lamichhane, D.R. & Read, J.C. (2017). Investigating children's passwords using a game based survey. *2017 Conference on Interaction Design and Children - IDC '17*, pp. 617-622.
18. Maqsood, S., Biddle, R., Maqsood, S., & Chiasson, S. (2018). An exploratory study of children's online password behaviours. In *17th ACM Conference on Interaction Design and Children (IDC '18)*. Association for Computing Machinery,
19. Mendori, T., Ikenoue, N., & Shimizu, A. (2005). Password input method using icons for primary school children. In C.-K. Looi et al. (Eds.), *Towards Sustainable and Scalable Educational Innovations Informed by the Learning Sciences.* Amsterdam: IOS Press.
20. Mendori, T. Kubouchi M., Okada, M. & Shimizu, A. (2002). Password input interface suitable for primary school children. In *International Conference on Computers in Education (ICCE'02).* IEEE, pp 765-766.
21. Office of Communication (Ofcom). (2018). Children and parents: Media use and attitudes report 2018. Available at https://www.ofcom.org.uk/ data/assets/ pdf_file/0024/134907 /Children-and-Parents-Media-Use-and-Attitudes-2018.pdf (Accessed: 23 January 2020)
22. Read, J.C. & Cassidy, B. (2012). Designing textual password systems for children. In *11th International Conference on Interaction Design and Children (IDC '12*).
23. Renaud, K. (2006). A visuo-biometric authentication mechanism for older users. In *People and Computers XIX—The Bigger Picture* (pp. 167-182). Springer, London.
24. Renaud, K. (2009). Web authentication using Mikon images. In *2009 World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09*). IEEE Computer Society, USA, 79–88.
25. Schwab, D., Alharbi, L., Nichols, O. & Yang, L. (2018). Picture PassDoodle: usability study. In *IEEE 4th International Conference on Big Data Computer Service and Applications*. IEEE.
26. United Nations Children's Fund (UNICEF). (2017). *The state of the world's children 2017: children in a digital world*. UNICEF.
27. Varenhorst, C. (2004). *Passdoodles: a lightweight authentication method.* MIT Computer Science and Artificial Intelligence Lab. Available at: https://pdfs.semanticscholar.org/ 8123/44ba01a9ed10db2ec3d17a56e852ac33cc78.pdf (Accessed: 23 January 2020)