Design and Evaluation of Graphical Authentication Systems for Arab Children

Esra Khalil Alkhamis

PhD

University of York

Computer Science

March 2023

Abstract

The increasing use of digital technologies by all ages means the number of online accounts used by children is also increasing. The COVID-19 pandemic further increased this situation with children staying at home to do schooling and communicate with friends online. It is thus urgent to investigate authentication systems for this age group. Text passwords are still the most used authentication systems, however children have a range of problems with them. Unfortunately, little research has investigated suitable authentication systems for children. The aim of this programme of research is to bridge this gap by investigating the usability of graphical authentication systems for children. The research is divided into three phases, each consisting of one or more studies that provide insight for the next phase. Phase 1 focuses on understanding and exploring password knowledge and practices of children who are native speakers of Arabic. This phase revealed a number of challenges for Arabic children with text passwords, due to their level of cognitive development and lack of literacy in the English language. In Phase 2 two graphical authentication systems, DoodlePass and ObjectPass, were designed and evaluated based on three usability aspects: effectiveness, efficiency, and satisfaction. The findings showed that both these systems are effective, efficient, and satisfying for Arab children aged 6 to 12 years, and promising alternatives for text passwords. Phase 3 compared the DoodlePass and ObjectPass authentication systems. The findings showed that ObjectPass is significantly more effective, efficient, and satisfying compared with DoodlePass. Both qualitative and quantitative analysis of the data were undertaken at all stages of the research. Overall, the findings suggest that graphical authentication systems are usable and promising alternatives for text passwords to overcome literacy and memorability challenges for children in the 6 to 12 years age group.

Table of Contents

ABSTRACT ..... **I**

TABLE OF CONTENTS ..... **II**

LIST OF FIGURES ..... **VIII**

LIST OF TABLES ..... **XI**

GLOSSARY ..... **XVI**

ACKNOWLEDGMENTS ..... **XVII**

DECLARATION ..... **XVIII**

CHAPTER 1 ..... **1**

INTRODUCTION **1**

1.1 RESEARCH MOTIVATION AND AIMS 2

1.2 RESEARCH APPROACH AND METHODOLOGY 4

1.3 RESEARCH CONTRIBUTIONS 7

1.4 ETHICAL STATEMENT 8

1.5 THESIS STRUCTURE 9

CHAPTER 2 ..... **10**

LITERATURE REVIEW **10**

2.1 INTRODUCTION 10

2.2 COGNITIVE DEVELOPMENT THEORY 11

2.3 EMPIRICAL RESEARCH ON AUTHENTICATION SYSTEMS FOR CHILDREN 14

2.4 INTERVIEW AND QUESTIONNAIRE RESEARCH ON AUTHENTICATION SYSTEMS FOR CHILDREN 37

2.5 RESEARCH ON GUIDELINES AND BEST PRACTICE FOR PASSWORDS FOR CHILDREN 43

2.6 CONCLUSIONS 48

CHAPTER 3 51

STUDY 1: EXPLORATORY STUDY OF CHILDREN'S UNDERSTANDING OF ONLINE SECURITY AND PASSWORDS 51

3.1 INTRODUCTION 51

3.2 METHOD 52

3.2.1 Design 52

3.2.2 Participants 53

3.2.3 Interview schedule 54

3.2.4 Procedure 58

3.2.5 Data preparation 59

3.3 RESULTS 61

3.3.1 RQ1: Do Saudi children use digital devices at home or at school? 61

3.3.1.1 Digital devices that children use 61

3.3.1.2 Digital devices and the use of passwords 62

3.3.2 RQ2: Do Saudi children understand the reasons for having passwords? 63

3.3.2.1 What children thought about password usage 63

3.3.2.2 Children's best practices while making passwords 65

3.3.2.3 Principles followed by children to create a password 77

3.3.2.4 Adults role in creating and managing children's passwords 79

3.3.3 RQ3: Do Saudi children have problems in relation to password creation in Latin alphabet and in English? *80*

3.3.4 RQ4: At what age do Saudi parents think it is important for their children to understand how to make passwords for online systems? *81*

3.4 DISCUSSION 82

3.4.1 Saudi children's use of password and digital devices at home and at school *82*

3.4.2 Saudi children's understanding of the reason for passwords and how to create them *82*

3.4.3 Saudi children and the use of Latin alphabet in password creation *85*

3.4.4 Saudi parent's opinion of the importance of their child understanding how to make passwords *86*

3.5 CONCLUSIONS 87

CHAPTER 4 88

STUDY 2: DOODLEPASS: AN AUTHENTICATION SYSTEM SUITABLE FOR CHILDREN 88

4.1 INTRODUCTION 88

4.2 METHOD 89

4.2.1 Design *89*

4.2.2 Participants *94*

4.2.3 Materials and equipment *96*

4.2.4 Procedure *105*

4.2.5 Data preparation and analysis *108*

4.3 RESULTS 115

4.3.1 DoodlePass Authentication System *115*

4.3.1.1 DoodlePass:1 116

4.3.1.2 DoodlePass:2 120

4.3.1.3 DoodlePass:3 126

4.3.2 Children's preferences between DoodlePass and a text password and memorability issues related to DoodlePass *133*

4.4 DISCUSSION 139

4.5 CONCLUSIONS 141

CHAPTER 5 142

STUDY 3: OBJECTPASS: AN AUTHENTICATION SYSTEM SUITABLE FOR CHILDREN 142

5.1 INTRODUCTION 142

5.2 METHOD 143

5.2.1 Design *143*

5.2.2 Participants *146*

5.2.3 Materials and equipment *147*

5.2.4 Procedure *154*

5.2.5 Data preparation and analysis *155*

5.3 RESULTS 159

5.3.1 ObjectPass Authentication System *159*

5.3.1.1 Candidate objects and key objects 159

5.3.1.2 ObjectPass:1 163

5.3.1.3 ObjectPass:2 166

5.3.1.4 ObjectPass:3 171

5.3.2 Children's preferences between ObjectPass and text passwords *175*

5.4 DISCUSSION 184

5.5 CONCLUSIONS 186

CHAPTER 6 187

STUDY 4: COMPARISON OF THE DOODLEPASS AND OBJECTPASS AUTHENTICATION SYSTEMS 187

6.1 INTRODUCTION 187

6.2 METHOD 188

6.2.1 Participants *188*

6.2.2 Data preparation and analysis *189*

6.3 RESULTS AND DISCUSSION 190

6.3.1 Comparison of DoodlePass and ObjectPass authentication systems on effectiveness and efficiency *190*

6.3.1.1 DoodlePass:1 vs ObjectPass:1 190

6.3.1.2 DoodlePass:2 vs ObjectPass:2 192

6.3.1.3 DoodlePass:3 vs ObjectPass:3 194

6.3.2 Children's preferences for DoodlePass or ObjectPass *197*

6.4 CONCLUSIONS 201

CHAPTER 7 203

GENERAL DISCUSSION AND CONCLUSIONS 203

7.1 INTRODUCTION 203

7.2 OVERVIEW OF THE PROGRAMME OF RESEARCH 204

7.3 CONTRIBUTIONS OF THE PROGRAMME OF RESEARCH 206

7.4 LIMITATIONS AND FUTURE WORK 207

7.5 CONCLUSIONS 209

APPENDIX A 210

APPENDIX B 222

APPENDIX C 227

REFERENCES 230

List of Figures

Figure 1.1 Phases of the programme of research 5
Figure 2.1 The three versions of the PassTiles authentication system (Source: Assal, Imran and Chiasson, 2018) 20
Figure 2.2 Storyboard template (Source: Chartofylaka & Delcroix, 2018).....22
Figure 2.3 Sample of storyboard (Source: Chartofylaka & Delcroix, 2018).....23
Figure 2.4 Sample of Android-pattern passcode (author's own drawing).....24
Figure 4.1 Overview of the design of DoodlePass authentication system.....93
Figure 4.2 Login distribution and authentication key in each session at DoodlePass authentication system 94
Figure 4.3 Username page for the DoodlePass authentication system 97
Figure 4.4 Authentication grid of 3 x 3 doodles for the DoodlePass authentication system (login page).....98
Figure 4.5 Authentication key registration pages in DoodlePass authentication system 99
Figure 4.6 Website page sequences for the DoodlePass authentication system 102
Figure 4.7 Website page sequences for Sessions 2 and 3 in the DoodlePass authentication system 103
Figure 4.8 Website page sequences for Sessions 4 and 5 in the DoodlePass authentication system 104
Figure 4.9 Error messages in the DoodlePass authentication system 108
Figure 4.10 Complete drawing that I split into three doodles as the child chose not to draw individual doodles (see text in section 4.2.5) 114
Figure 4.11 Median times and semi interquartile ranges for successful first logins for DoodlePass:1 116
Figure 4.12 Median times for successful first logins for DoodlePass:1 for Session 1, Login 2 for children in each grade 118
Figure 4.13 Median times for successful first logins for DoodlePass:1 for Session 2, Login 1 for children in each grade 119
Figure 4.14 Median times for Session 2 and Session 3 logins for DoodlePass:2 121
Figure 4.15 Overall median times and semi interquartile ranges for DoodlePass:2 122
Figure 4.16 Median times for successful first logins for DoodlePass:2 for Session 2, Login 3 for children in each grade 124

Figure 4.17 Median times for successful first logins for DoodlePass:2 for Session 3, Login 1 for children in each grade (no SIQR for grade 4 as only two values) 125
Figure 4.18 Median times for successful first logins for DoodlePass:2 for Session 3, Login 2 for children in each grade (no SIQR for grade 4 as only four values) 126
Figure 4.19 Median times for Session 3, Session 4, and Session 5 logins for DoodlePass:3 129
Figure 4.20 Overall median times and semi interquartile ranges for DoodlePass:3 129
Figure 4.21 Median times for successful first logins for DoodlePass:3 for Session 3, Login 3 for children in each grade (no SIQR for grade 4 as only two values) 132
Figure 5.1 Overview of the design of ObjectPass authentication system 145
Figure 5.2 Authentication grid of 3 x 3 objects for ObjectPass authentication system (login page) 148
Figure 5.3 Object Registration pages for ObjectPass authentication system 149
Figure 5.4 Key Registration pages in ObjectPass authentication system 150
Figure 5.5 Website page sequences for Session1 in the ObjectPass authentication system ..153
Figure 5.6 Median times for candidate object 3 for children in each grade 161
Figure 5.7 Median times and semi interquartile ranges for successful first logins for ObjectPass:1 163
Figure 5.8 Median times for successful first logins for ObjectPass:1 for Session 1, Login 1 for children in each grade 165
Figure 5.9 Median times for Session 2 and Session 3 logins for ObjectPass:2 167
Figure 5.10 Overall median times and semi interquartile ranges for ObjectPass:2 167
Figure 5.11 Median times for successful first logins for ObjectPass:2 for Session 2, Login 3 for children in each grade 169
Figure 5.12 Median times for successful first logins for ObjectPass:2 for Session 3, Login 2 for children in each grade 170
Figure 5.13 Median times for Session 3, Session 4, and Session 5 logins for ObjectPass:3 .172
Figure 5.14 Overall median times and semi interquartile ranges for ObjectPass:3 172
Figure 5.15 Median times for successful first logins for ObjectPass:3 for Session 3, Login 3 for children in each grade 174
Figure 6.1 Mean login times (and standard deviations) for all attempts in DoodlePass:1 vs ObjectPass:1 192
Figure 6.2 Mean login times (and standard deviations) for all attempts in DoodlePass:2 vs ObjectPass:2 193

Figure 6.3 Mean login times (and standard deviations) for all attempts in DoodlePass:3 vs ObjectPass:3 195

List of Tables

Table 2.1 Percentage of children using Internet in Saudi Arabia (Source: General Authority for Statistics, 2017, 2018) 10
Table 2.2 Summary of the empirical research on graphical authentication systems for children 31
Table 2.3 summary of the interview and questionnaire research on authentication systems for children 42
Table 2.4 Password best practice for children of different ages (Prior & Renaud, 2020) 43
Table 2.5 Guidelines for designing graphical authentication mechanisms for pre-literate children (Stewart et al., 2020) 45
Table 3.1 Gender and school grade/age breakdown of the children interviewed in Study 1 ..53
Table 3.2 Mapping interview questions to the research questions in Study 1 55
Table 3.3 Use of different types of digital devices at home and at school 61
Table 3.4 Activities with digital devices at home (N=39) 62
Table 3.5 Thematic analysis of answers to Q25. (Why do people have passwords?) (N = 37) 64
Table 3.6 Security words used in Q25 (Why do people have passwords?) (N = 10) 65
Table 3.7 Grade distribution of children who have passwords (N = 29) 65
Table 3.8 Reasons given for Q26. (Why do you think that strong passwords are used in real life?) (N = 38) 67
Table 3.9 Security words used in Q26 (Why do you think that strong passwords are used in real life?) (N = 6) 68
Table 3.10 Analysis of the composition of easy and hard passwords created by the children in Study 1 69
Table 3.11 Password strength of children's hard passwords created in Study 1 70
Table 3.12 Analysis of easy passwords by children's school type 70
Table 3.13 Analysis of hard passwords by children's school type* 71
Table 3.14 Analysis of easy passwords by children's grade 72
Table 3.15 Analysis of hard passwords by children's grade. * 73
Table 3.16 Thematic analysis of children's reasons for why the password they created is easy (N=39). 74
Table 3.17 Comparison of children's easy passwords to their explanatory answers (Why it was an easy password?) by children's grade. 75

Table 3.18 Thematic analysis of children's reasons why the password is hard (N=37).....76
Table 3.19 Comparison of children's hard passwords with their explanatory answers (Why it was hard password?) by children's grade.....77
Table 3.20 Children's selection of what makes a good password (N = 39) 78
Table 3.21 Children's selection of what makes a good password by school type.....78
Table 3.22 Children's selection of what makes a good password by grade 78
Table 3.23 Children's use of the Internet with or without parental help by grade 79
Table 3.24 Parental login for their child by children's school type* 79
Table 3.25 Parental login for their child by children's grade 79
Table 3.26 Parental creation of passwords for their child by children's school type* 80
Table 3.27 Parental creation of passwords for their child by children's grade.....80
Table 3.28 Parent's answers on number of English words known by children in the study (N=39) 81
Table 3.29 Parents' opinion of the importance of their child understanding how to make a password for online system by children's grade 81
Table 4.1 Distribution of participants in Pre-Session and Sessions 1 to 4 for the DoodlePass authentication system 95
Table 4.2 Distribution of participants in Session 5 for the DoodlePass authentication system 95
Table 4.3 Open ended questions asked in each experimental session 101
Table 4.4 Categories of doodles with examples used in DoodlePass authentication system 111
Table 4.5 Cases of doodle re-categorisation in DoodlePass authentication system 113
Table 4.6 Number of participants who withdrew for each session about the DoodlePass authentication system 115
Table 4.7 Accuracy and median times for login with DoodlePass:1.....116
Table 4.8 Kruskal-Wallis tests of grade differences in DoodlePass:1 login times.....118
Table 4.9 Mann-Whitney tests of differences between grades in DoodlePass:1 login times for Session 1, Login 2 (each grade compared to the previous grade) 119
Table 4.10 Mann-Whitney tests of differences between grades in DoodlePass:1 login times for Session 2, Login1 (each grade compared to the previous grade) 120
Table 4.11 Number of participants in DoodlePass:2 sessions 120
Table 4.12 Accuracy and median times for login with DoodlePass:2.....121
Table 4.13 Kruskal-Wallis tests of grade differences in overall DoodlePass:2 login times..123

Table 4.14 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 2, Login 3 (each grade compared to the previous grade) 124
Table 4.15 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 3, Login1 (each grade compared to the previous grade) 125
Table 4.16 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 3, Login2 (each grade compared to the previous grade) 126
Table 4.17 Number of participants in DoodlePass:3 sessions 127
Table 4.18 Accuracy and median times for login with DoodlePass:3 127
Table 4.19 Wilcoxon tests of differences in overall login times between successive logins for DoodlePass:3 131
Table 4.20 Kruskal-Wallis tests of grade differences in overall DoodletPass:3 login times.131
Table 4.21 Mann-Whitney tests of differences between grades in DoodlePass:3 login times for Session 3, Login 3 (each grade compared to the previous grade) 132
Table 4.22 Number of children who have more than one attempt while using DoodlePass:3 authentication system for each grade.....133
Table 4.23 Breakdown of preference for DoodlePass and text password for ease of remembering by children's grade (N = 37) 133
Table 4.24 Breakdown of preference for DoodlePass and text password by children's grade (N = 37) 134
Table 4.25 Breakdown of preference for two or three doodles in DoodlePass for ease of remembering by children's grade (N = 27) 135
Table 4.26 Breakdown of ease of remembering DoodlePass for long time by children's grade (N = 27) 135
Table 4.27 Breakdown of difficulty level to remember DoodlePass by children's grade (N = 22).....136
Table 4.28 Breakdown of preference for DoodlePass and text password for ease of remembering by children's grade (N = 22) 137
Table 4.29 Breakdown of preference for DoodlePass and text password by children's grade (N = 22) 138
Table 4.30 Reasons given for how children remembered their DoodlePass after 9 months (N = 19).....138
Table 5.1 Distribution of all participants for ObjectPass authentication system 146
Table 5.2 Distribution of new participants and participants who had participated in DoodlePass and ObjectPass authentication systems 147

Table 5.3 Open ended questions asked at each experimental session 152
Table 5.4 Categories of objects with examples used in ObjectPass authentication system ..157
Table 5.5 Median times for selecting candidate objects 160
Table 5.6 Kruskal-Wallis tests of grade differences in overall choosing candidate objects times.....160
Table 5.7 Mann-Whitney tests of differences between grades in time to choose object for candidate object 3 (each grade compared to the previous grade).....161
Table 5.8 Median times for selecting Key objects.....162
Table 5.9 Kruskal-Wallis tests of grade differences in overall choosing key objects times .162
Table 5.10 Accuracy and times for login with ObjectPass:1.....163
Table 5.11 Kruskal-Wallis tests of grade differences in ObjectPass:1 overall login times...164
Table 5.12 Mann-Whitney tests of differences between grades in ObjectPass:1 login times for Session 1, Login 1 (each grade compared to the previous grade) 165
Table 5.13 Accuracy and times for login with ObjectPass:2.....166
Table 5.14 Kruskal-Wallis tests of grade differences in overall ObjectPass:2 login times...168
Table 5.15 Mann-Whitney tests of differences between grades in ObjectPass:2 login times for Session 2, Login3 (each grade compared to the previous grade) 169
Table 5.16 Mann-Whitney tests of differences between grades in ObjectPass:2 login times for Session 3, Login 2 (each grade compared to the previous grade) 170
Table 5.17 Accuracy and times for login with ObjectPass:3.....171
Table 5.18 Wilcoxon tests of differences in overall login times between successive logins for ObjectPass:3 173
Table 5.19 Kruskal-Wallis tests of grade differences in overall ObjectPass:3 login times...174
Table 5.20 Mann-Whitney tests of differences between grades in ObjectPass:3 login times for Session 3, Login 3 (each grade compared to the previous grade) 175
Table 5.21 Number of children with more than one attempt while using ObjectPass authentication system for each grade.....175
Table 5.22 Grade breakdown of types of people mentioned in relation to why the child has a password (N= 107) 177
Table 5.23 Reasons given for why you use a password (N = 101).....178
Table 5.24 Security words used in Q2. Why do you use a password? (N=31*) 179
Table 5.25 Grade breakdown of security words used in Q2. Why do you use a password (N=31)?.....179

Table 5.26 Breakdown of answers to Q3 (Which is easier to remember ObjectPass or text password?) by children's grade (N = 52) 180
Table 5.27 Reasons given for thinking ObjectPass or a text password is easier to remember (N = 45) 181
Table 5.28 Breakdown of answers to Q4 (Which is more preferred ObjectPass or text password?) by children's grade (N = 52) 182
Table 5.29 Reasons given for preferring ObjectPass or text password (N = 48) (* = new category from Table 5.26) 183
Table 6.1 Distribution of participants who had participated in both systems 188
Table 6.2 Accuracy of DoodlePass1 and ObjectPass:1 (mean number of attempts required) 191
Table 6.3 Mean Login times (and standard deviations) for DoodlePass:1 and ObjectPass:1* 191
Table 6.4 Accuracy of DoodlePass:2 and ObjectPass:2 192
Table 6.5 Mean login times (and standard deviations) for DoodlePass:2 and ObjectPass:2 .193
Table 6.6 Accuracy of DoodlePass:3 and ObjectPass:3* 194
Table 6.7 Login times for DoodlePass:3 and ObjectPass:3 across sessions* 195
Table 6.8 Preference for DoodlePass or ObjectPass for ease of remembering by children's grade 197
Table 6.9 Reasons given for thinking DoodlePass or ObjectPass is easier to remember (N = 21) 198
Table 6.10 Preference for DoodlePass and ObjectPass by children's grade 199
Table 6.11 Reasons given for preferring DoodlePass or ObjectPass (N = 21) (* = new category from Table 6.9) 200

Glossary

Authentication key – Set of images used to authenticate.

Entropy – a measure of how unpredictable a password is.

DoodlePass:x – Authentication with the (first, first and second, or all three) doodles that the child created in the Pre-Session.

DP:xGy - DoodlePass (1, 2 or 3) doodles, Grid (1, 2 or 3)

ObjectPass:x – Authentication with the (first, first and second, or all three) objects that the child chooses in Session 1.

OP:xGy - ObjectPass (1, 2 or 3) objects, Grid (1, 2 or 3)

Acknowledgments

First, I would like to thank Allah for guiding me and granting me success in my scientific journey, through which I hope to spread knowledge to humanity.

Special thanks go to my supervisor, Prof. Helen Petrie. With your continuous support and guidance, I was able to achieve my goal. Your concern for the accuracy and quality of my work were the most important pillars of my scientific journey. Prof. Helen, I'm proud to have you as a supervisor!

I extend my thanks to my examiners, Dr. Siamak Shahandashti and Dr. Gavin Sim, for their distinguished and enriching management of my PhD viva, which produced essential comments that reflected positively on the content of this thesis.

This work would not have been successful without encouragement and prayers from my parents, Prof. Khalil and beloved Karemah. You are my greatest inspiration. You made me believe that I could complete this journey successfully. Thank you for being in my life and for everything you have done to smooth the road on this journey.

To my dearest husband, Ramy, thank you for the immense love and support you provided from the start of this journey to the final minute of my thesis submission. My beloved angels, Nawaf, Asma and Saud, your laughter and humour were the fuel that gave me the strength to accomplish my goal. I love you, my sunshine!

I am grateful for all my siblings who encouraged and supported me, especially my brother Mosab and my sister, my twin soul, Asma. Asma, you are always by my side to motivate and uplift me in times of sadness. I'm lucky to have you as a sister and best friend!

My final acknowledgements go to all the parents and children who participated in this study and to King Saud University and the External Joint Supervision Programme for funding this scholarship.

Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Some of the material contained in this thesis has appeared in the following published paper:

Alkhamis, E., Petrie, H., & Renaud, K. (2020). KidsDoodlePass: an exploratory study of an authentication mechanism for young children. In N. Clarke, & S. Furnell (Eds.), *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings* (pp. 123-132). (IFIP Advances in Information and Communication Technology (IFIPAICT); Vol. 593). Springer. https://doi.org/10.1007/978-3-030-57404-8_10

Chapter 1

Introduction

Nowadays, digital technologies are very used widely, this results in increased numbers of online accounts that users need to manage. Each of these accounts requires the use of authentication credentials: usually a username and password. The most used form of authentication mechanism is still a text password that uses the Latin alphabet. Unfortunately, people in different age groups such as children, older people and people with disabilities, struggle with text passwords, this triggered researchers to investigate suitable solutions. However, most of this research and the solutions have focused on adults, while little research in this area has focused on children and their particular needs.

Children are important segment and form a quarter of the world's population (Statista Research Department, 2022). Mark McCrindle, an Australian social researcher, suggested the term "Generation Alpha" for children since 2010 (Ziatdinov and Cilliers, 2021). This generation has been exposed to digital technologies from a very young age (Amrit, 2020), and have more access to information than previous generations (McCrindle and Fell, 2020). The idea of changing adult's technologies to be suitable for children, might be not ideal solution (Read & Markopoulos, 2013). This raises the importance to have digital technologies designed and evaluated with respect to children needs and to involve them in the design of these technologies (Dempsey et al., 2016).

The field of Child Computer Interaction (CCI) is a growing part of Human Computer Interaction (HCI) (Dempsey et al., 2016). It includes Child Centred Security (CCS) which in turn includes authentication systems. Since Generation Alpha have more access to digital technologies, this leads to a greater need to use authentication systems to access their devices, data and accounts. This programme of research focuses on usable authentication system for children by understanding the current knowledge and behaviour of young Arab children in relation to digital security and authentication. This will enable me to suggest alternative authentication systems for young children in general, but specifically grounded within the Arab cultural context.

2.1 Research Motivation and Aims

Typically, computer users use one or more of the three traditional authentication ways: 1) something you know, 2) something you have, and 3) something proves who you are.

The most commonly used form of authentication is "*something you know*" text password. Considerable research has been conducted in the field of text password for adults over the last 20 years. In line with this research, researchers have proposed alternative authentication systems to replace text passwords suitable for adult to overcome usability and security problems. On the other hand, for children only a little research has been conducted and most it is for native English speakers. Stewart et al (2020) summarize the major problem for children with text passwords, that their literacy affects children's ability to parse words into letters. In addition, the standard QWERTY keyboard is able to produce capital letters but when pressed by a child it will produce lowercase letters by default and provide no feedback or confirmation of what they have typed for their text password. Moreover, with literacy issues and memory for text password, Sowell et al. (2004) state that children do not have the same level of memory retention as adults until they reach adolescence. This reflects a difficulty for children to retain their text passwords for long time due to their level of cognitive ability. Children with dyslexia (Peyrin et al., 2012) are even more vulnerable to problems with text passwords because of their difficulties in reading, writing, and spelling. In addition, as a text password needs to be secret and not shared, children in their normal lives are not necessarily able to distinguish between people with whom they can share their secrets, and those with whom they should not (Anagnostaki et al., 2013). Finally, for text password entry, adults have to track mentally the position of each character in their text password, children's ability to do so is low due to their short attention span and different abilities to focus on a specific task for a period of time (Stewart et al, 2020).

In addition to these difficulties that all children have with text passwords, Arab children who are not native English speakers and who do not use Latin alphabet in their native language have even more challenges with text passwords due to language differences. Specifically, because many authentication systems used in the Arab world require a text password in the Latin alphabet, their ability to create a text password using the Latin alphabet, spell their text password on repeated occasions, and use a keyboard with the Latin alphabet is less than other children who use the Latin alphabet in their daily lives (see Chapter 3, section 3.4.3). To date

and to the best of my knowledge, no research has been conducted to explore text password knowledge and best practices for children who are native speakers of Arabic.

Therefore, asking children to use text password before they are mentally and cognitively ready is not recommended. For the other form of authentication "*something you have",* which requires the user to have a token of some kind, is unlikely to be useful with young children. Asking them to have a token and remember how to use it is probably beyond their cognitive abilities. For "*something proves who you are*", it has been suggested that using a child's biometrics would be useful for children with disabilities (Anna & Theng, 2011), however important privacy issues need to be considered for children (Darroch, 2011; Dixon, 2017). Additionally, biometric readers are not as universally used as keyboards and touchscreens.

A solution investigated in this thesis to overcome these challenges for children is the use of authentication system that relies on children's capability for recognition rather than recall. This can be achieved by the use of graphical authentication systems.

To achieve this overall aim of the programme of research presented in this thesis, the main research question for the thesis is:

Are graphical authentication systems usable and acceptable for young Arab children?

This thesis is divided into three phases: in Phase 1, the aim is to understand and explore password knowledge and practices for children who are native speakers of Arabic (see Study 1, Chapter 3). This research addresses the following research questions

RQ1: Do Saudi children use digital devices at home or at school?

RQ2: Do Saudi children understand the reasons for having passwords and how to create good ones?

RQ3: Do Saudi children have linguistic problems in relation to password creation in the Latin alphabet and in English?

RQ4: At what age do Saudi parents think it is important for their children to understand how to make passwords for online systems?

In Phase 2, the aim is to overcome challenges identified in Phase 1, that children have with text passwords. This is done by designing and evaluating two graphical authentication systems suitable for young children. The first, DoodlePass authentication system, involved children creating three doodles themselves to use as their authentication key. The second, ObjectPass authentication system, involved children using images of objects as their authentication key. This research addresses the following research questions:

In Study 2, Chapter 4:

RQ5: Is the DoodlePass authentication system usable by children aged 6 to 12 years?

In Study 3, Chapter 5:

RQ6: Why do children think they need a password? (investigated again with different participants in this study)

RQ7: Is the ObjectPass authentication system usable by children aged 6 to 13 years?

In Phase 3, the aimed to compare the usability aspect of both systems in term of effectiveness, efficiency, and satisfaction. This addresses the following research questions (see Study 4, Chapter 6):

RQ8: Which system was more usable, the DoodlePass authentication system or the ObjectPass authentication system?

RQ9: Does children's age affect their performance and attitudes towards the DoodlePass authentication system and the ObjectPass authentication system?

2.2 Research Approach and Methodology

In the programme of research presented in this thesis, the main research question has been addressed by breaking the research into three phases (see Figure 1.1).

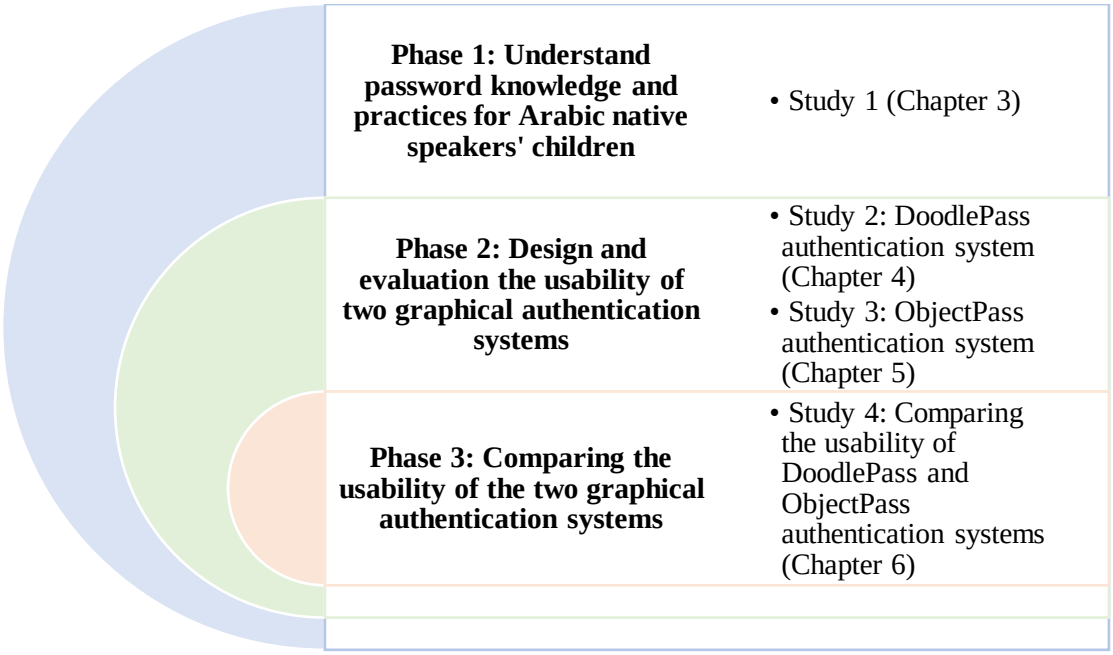


Figure 2.1 Phases of the programme of research

The research in Phase 1 started with exploratory study (Study 1, Chapter 3) used semi-structured interviews, conducted face to face (except for one interview though a facetime video call). 39 Saudi children aged 6 to 12 years participated on this study with one of their parents (the child's mother in all cases). The interview comprised closed and open-ended questions and was divided into three sections: demographic questions, questions for the parent, and questions for the child. The aim of this study is to understand children's knowledge and security practices with regard to text passwords, such as their level of understanding of the need for passwords and their ability to create and explain a weak and a strong password. Both qualitative and quantitative analysis of the data were undertaken. The results show that children have a good understanding of security best practices, but they struggle to apply this understanding correctly perhaps due to their cognitive capabilities that are not yet fully developed. In addition, Arabic children have more challenges due to their lack of literacy in the English language. Therefore, it was important to investigate alternative authentication systems suitable for children, particularly ones which do not depend on text input.

Following this exploratory study, in Phase 2, in Study 2 (Chapter 4) a graphical authentication system called DoodlePass was designed and evaluated with 37 Saudi children aged 6 to 12 years. 15 children withdrew gradually in the last three sessions due to the COVID-19 pandemic; this meant that 22 children completed this study. The DoodlePass authentication system is a web-based system that uses children's own drawings (doodles) as an authentication

key instead of a text password. In the most complex form of the system, children need to recognise their three doodles at the correct order from among of other children's doodles in order to authenticate themselves and log in into a system where they can play games. The study used a mixed design, with one between-participants independent variable (school grade) and two within-participants independent variables (complexity of the DoodlePass authentication system and login occasion to recognise and selecting DoodlePass). It consisted of five sessions, four sessions were conducted face-to-face with children at quiet room at their school, but Session 5 was conducted online via Zoom due to the COVID-19 pandemic. The DoodlePass authentication system was evaluated in term of effectiveness, efficiency, and satisfaction for short-, medium-, and long-term memorability. Both qualitative and quantitative analysis of the data. The results show that most children recognised and were able to select their DoodlePass doodles in the correct order and the majority of children preferred to use DoodlePass authentication system in comparison with a text password.

A second study was conducted in Phase 2, (Study 3, Chapter 5). After the promising results of Study 2 another graphical authentication system designed, ObjectPass authentication system. This authentication system uses images of objects familiar to young children as the authentication keys. This is to make the system easier to use by developer, using of objects are less complicated process than collecting doodles from children and insert it manually to the system. Furthermore, to ensure children satisfaction as it is reported in (Study 2, Chapter 4) not all children prefer to draw. The ObjectPass authentication system was evaluated with 52 Saudi children aged 6 to 13 years. This study was conducted totally online through Zoom due to the COVID-19 pandemic. 21 of the children who participated in this study had participated in the previous study with the DoodlePass authentication system and this was intentional to allow the comparison between the two systems. The design of this study and evaluation measures were the same as those in Study 2. The results show that in the most complex version of the system all children were able to recognise their ObjectPass images and select them in the correct order and the majority of children preferred to use ObjectPass in comparison with a text password.

Phase 3 aimed to conduct further analyses to compare the DoodlePass and ObjectPass authentication systems. Data from the 21 Saudi children aged 6 to 12 years who took part in both Studies 2 and 3 were analysed, as they had used both the DoodlePass and ObjectPass authentication systems. Both qualitative and quantitative analysis of the data were undertaken. In this analysis I chose to use parametric statistics, due to reasons discussed in (Chapter 6,

session 6.2.2), in particular analysis of variance (ANOVA), using the Greenhouse-Geisser adjustment of degrees of freedom to account for issues of non-homogeneity of variance. In addition, key significant results were checked with non-parametric statistics and only included if they were also significant with both parametric and non-parametric statistics. The results show that the ObjectPass authentication system is significantly more effective, efficient, and satisfying for children than the DoodlePass authentication system.

The main differences between the studies presented in this thesis and previous research discussed in the literature review (Chapter 2) are: first, participants in all studies were Arabic speaking Saudi children. Secondly, for Study 2 (Chapter 4) the DoodlePass authentication system, at the time of design and evaluation, as far as I know, was the first graphical authentication system to uses doodle with children in the age group 6-12 years, as only one small study (Renaud, 2009) had evaluated graphical authentication system using doodles with one grade of children (aged 11-12 years). Thirdly, Studies 2 and 3 (Chapter 4 and 5) evaluated both the Doodle and Object pass authentication systems in depth in terms of children's ability to remember their authentication key at different period of times. Fourthly, the ecological validity of Studies 2 and 3 can be considered high in terms of measuring the usability for each system alone without asking the children to remember more than one authentication key at the same time which is unrealistic. It is also important to note that all the studies in Phase 2 were designed between 2019 and early of 2020 which meant the designs were based on research published in early 2020 and before (see Table 2.2 for a list of research papers used in both studies).

2.3 Research Contributions

This research has several contributions to the development and evaluation of children's authentication system in the field of usable security and Child Centred Security (CCI). The main contributions in this research are:

- Development of an understanding of young Arab children's knowledge about security and best practices in relation to text passwords (as far as I am aware, this was the first such study on this topic that involves children whose first language is Arabic).

- Design, implementation, and evaluation of two graphical authentication systems suitable for young children aged 6 to 12 years (DoodlePass and ObjectPass authentication systems). Evaluation of both systems showed that these systems are effective and efficient, and a promising alternative to text passwords to overcome literacy and memorability challenges for this age group.

2.4 Ethical Statement

All studies conducted in this thesis were ethically approved by the Physical Sciences Ethics Committee of the University of York. Furthermore, my supervisor Prof. Helen Petrie, has an enhanced Disclosure and Barring Service (DBS) clearance to work with vulnerable groups including children. All studies adhered to the following ethical considerations: "Do No Harm", "Confidentiality", and "Informed Consent".

Do No Harm. None of the children participating in any studies was exposed to harmful or risky situations. In Study 1, children were asked to create passwords but before they did it was explained to them that they should not use a password that they used in real accounts nor should they use this created password in their real accounts.

Confidentiality. All collected data were anonymised, and only myself and my supervisor have access to this data. In addition, data are stored in password protected software on a password protected computer. All participants were assigned a unique code when referring to in the result sections of the thesis. To ensure confidentially of participants, for any password created in Study 1 which contained information that might reveal the identity of the participant, this information is hidden (e.g., if the password contains child's name, I removed his name and write instead "ChildName"). As the participants in all studies in this thesis are children, they were under the supervision of their parent (in Studies 1 and 3) or a teacher at the school (in Study 2).

Informed Consent. All parents of children were given a consent form to sign before starting the study. The consent form contained aim of the study, tasks to be done by the child, duration of the study, when I would be meeting the child, confidentiality of information, contact information, the right to withdraw from the study in any time, and the amount of the voucher that the child would receive upon completing the study. Furthermore, studies were explained verbally to the children and I confirmed with them that no data would be collected without the

permission from the child themselves and they were not obliged to do any of the tasks if they did not wish.

2.5 Thesis Structure

The upcoming chapters in this thesis will be as follows: Chapter 2 contains the literature review. Then Chapter 3 presents Study 1, the semi-structured interview regarding security knowledge and best practices with text password. Chapter 4 presents Study 2 on the DoodlePass authentication system. Chapter 5 presents Study 3 on the ObjectPass authentication system. Chapter 6 presents the comparison of the DoodlePass and ObjectPass authentication systems. Finally, Chapter 7 presents a final discussion of all studies presented in the thesis, discusses suggested future work and limitations of the research and draws final conclusions.

Chapter 2

Literature Review

3.1 Introduction

Children are not like adults in their thinking and memory capacities, so their behaviour in relation to technology and online accounts will undoubtedly be different. As expected, the number of children using technology and Internet is increasing yearly. In fact, the number increased sharply since the start of 2020 as a response to the lockdown due to the COVID-19 pandemic. This affected schooling and resulted in changing study mode to online from home. UNICEF (2017) estimates that for each three adult Internet users in the world, there is one child using the Internet. They also estimate that there is a steady increase of Internet usage among children and, in some countries, children are as likely to use Internet as adults above the age of 25. In a study published by the Government of Saudi Arabia (General Authority for Statistics, 2017, 2018)[1], for a sample of the main areas in Saudi Arabia, Internet usage for children up to the age of 19 years has surprisingly increased nearly fivefold between 2017 and 2018, as shown in Table 2.1. Similarly, studies in UK conducted by Ofcom (2021, 2022) show that nearly all children in the UK are using the Internet.

Table 3.1 Percentage of children using Internet in Saudi Arabia (Source: General Authority for Statistics, 2017, 2018)

Age/Year	2017	2018	Percentage Increase
0-4	0.65%	4.83%	643.1%
5-9	4.25%	23.44%	451.5%
10-14	7.50%	48.45%	546.0%
15-19	11.93%	89.13%	647.1%

[1] After 2018, the General Authority for Statistics did not publish information related to children aged 0-14.

The following sections explain children's cognitive development and present research conducted in the areas of usability and security of children's authentication mechanisms.

3.2 Cognitive development theory

As noted, children do not have the same cognitive and reasoning abilities as adults, these take some time to develop and go through a number of stages before reaching adult levels. It is surprising that the research on children's understanding and use of passwords and authentication systems has paid little attention to the stages of children's cognitive and reasoning development, as we need to consider how children of different ages will understand passwords and authentication.

One of the most widely used and respected theories of children's cognitive development is that of Jean Piaget (Miller, 2011). He argued that children go through four stages of cognitive development to reach adult levels. Children may go through the stages more or less quickly, at earlier or later ages, but they always follow this sequence and cannot miss stages. The stages he proposed are:

Sensorimotor stage (from birth to approximately two years of age): children in this stage can differentiate themselves from other objects. During this stage children acquire the concept of "object permanence" in which they learn that objects still exist even if they cannot not see them. So, very young infants express surprise if you hide a toy under a blanket and then show it again – their view of the world is that when the object disappears, it no longer exists. The fact that it reappears is a surprise. At a certain point, through enough examples, infants understand that objects continue to exist even if they cannot be seen.

Preoperational stage (approximately 2 to 7 years of age): during this stage children learn language and how to represent objects using images and words, which gives them important tools for cognition and reasoning. However, children at this stage have difficulty to understand the viewpoint of other people. Piaget's famous example to illustrate this difficulty is the three mountains task: children are shown a physical model of three mountains of different heights, with different objects on the top of each mountain. A doll is placed at different positions in relation to the model and children are asked to choose a photograph which shows what the doll can see. At this stage children they cannot imagine themselves in the position of the doll and

will be likely to choose a photograph showing what they themselves can see, this is called "egocentric" reasoning.

Concrete operational stage (approximately 7 to 11 years of age): during this stage children think in terms of concrete objects and specific instances, rather than abstract concepts. However, they do start to think logically about objects and events and start to understand the concept of "conservation", which in Piaget's theory refers to the fact that things can be organized in different ways, but remain the same. The famous example in this instance is pouring quantity of water from a short, wide glass to a tall, thin glass. If no water is spilled, the quantity of water remains the same, even if it looks more in the tall glass than in the wide glass (of course, even adults sometimes make mistakes in relation to conservation).

Formal operational stage (11 years to adulthood), from about the age of 11, children start to think and reason in the full adult way, to be able to manipulate abstract concepts, use logic and problem solve in an adult manner.

Piaget's theory is not without its critics and adaptations e.g., work by Bruner (see Smorti & Fioretti, 2019) and Kohlberg (see Crain 1985). However, a more recent extension of Piaget's thinking about the preoperational stage which is particularly important for the study of authentication systems for children, is the "theory of mind" concept developed by Baron-Cohen et al. (1985) in relation to cognitive development, particularly in relation to children who may be autistic. This concept refers to the fact that very young children at this stage do not understand what other people will know or believe or not (as opposed to just see or not see, which was the emphasis of Piaget's interest). The theory of mind can be illustrated with a task similar to the three mountains, called the Sally Anne task. Children are shown interaction between two dolls - Sally and Anne, who have a basket and a box, respectively. Sally also has a marble, which she places into her basket, and then leaves the room. While she is out of the room, Anne takes the marble from the basket and puts it into the box. Sally returns, and the child is then asked where Sally will look for the marble. Children at the preoperational stage will answer that Sally will look in the box, as they do not yet understand that Sally will not know that Anne has moved the marble. They do not understand that another's mental representation of the situation is different from their own, and they cannot predict behaviour based on that understanding. Baron-Cohen et al. argue that autistic children fail to move on and develop a "theory of mind" which allows them to understand what different people will know or believe, depending on the information they have.

However, for children's understanding and use of authentication systems and passwords, what is important to take from "theory of mind" is that young children may not have developed the concept of keeping things secret from people. Children at the preoperational stage will not necessarily understand that they may know their password, but that other people will not know that information, so it is a secret. The idea of people trying to access that information will be difficult them to understand.

In this literature review, research papers published between 2002 and 2022 in the field of children's authentication systems and intentionally I omit research papers about systems for adults due to a number of factors. Firstly, in designing graphical authentication systems for adults, usability and security aspects need to be balanced such that high risk data should be secure enough, and this is not applicable in systems for children. Read and Cassidy (2012) suggested using shorter passwords for children as they are still learning how to use authentication system correctly and how to follow security aspects. In fact, children in this age group do not have sensitive or confidential information that they need to secure it as they are still under the supervision of their parents, therefore, we can minimize the concerns about security factors for children while concentrating on usability Choong (2019a). Secondly, children need specific type of images that are familiar to them and the images used with adults (e.g., different buildings) could not be recognised easily by children as suggested by Assal et al. (2018) and Renaud et al. (2021). Thirdly, systems designed specifically for children are not the same as those designed for adults, they have different accessibility issues (Assal et al., 2018) (e.g., children tend to use touchscreens instead of a mouse to drop and drag and to choose images, the interface appearance and the use of colours, children are ignorant about system notifications). Fourthly, research has shown that the ways adults memorise their authentication keys are different from those of children, so we cannot rely on systems built specifically for adults as a guide (Assal et al., 2018; Lamichhane and Read, 2017).

These research papers can be categorised into three types based on the work presented: papers that implement a system and test it with children (Empirical research on authentication systems for children); papers that did interviews or a survey with children (Interview and questionnaire research on authentication systems for children); and papers that suggest best practices and guidelines for children's passwords (Research on guidelines and best practice for passwords for children).

3.3 Empirical research on authentication systems for children

The earliest study related to passwords and children I could find was conducted by Mendori et al. (2002) with Japanese primary school age children. These researchers argued that not all children of this age know the Latin alphabet, so they proposed an authentication interface based on icons rather than letters. First, they investigated children's ability to distinguish between different kinds of icons. They presented 31 first grade children with examples of 10 different categories of icons (e.g., fruits, flowers, insects). The children were asked to describe the icons, to ensure that the children could discriminate between them. From this exercise, 65 types of icons which the children could discriminate were selected, which were then used in the password interface. As children of this age can use a mouse, the interface consisted of a number of icons which the user clicks with the mouse. An evaluation of this type of interface was conducted by testing three versions of the interface: one displaying 8 icons, one with 16 icons, and one with 64 icons. Almost all participants memorized their password, however many mistakes in input order were made. The second interface, with 16 icons, was the quickest to use.

Mendori et al. (2005) improved on their first password interface by changing the placement of buttons and making the icons bigger. In a further evaluation, Grade 2 children tested two different button arrangements from each of the following: 8 buttons, 12 buttons and 16 buttons. The 12 buttons interface produced the most correct entries, although not surprisingly the 8 buttons interface was the quickest to use.

Renaud (2009a) assessed the viability of using children's own drawings (Mikon) as an authentication system. A class of 24 children aged 11 - 12 participated in an experiment to investigate this idea. The children were asked to complete homework uploaded in an online system. In order to access their homework, they needed to be authenticated using the Mikon authentication system which consisted of three main phases: enrolment, authentication, and replacement. In the enrolment phase, children were added to the system by their teacher using the children's names and emails and then the teacher explained how to use the system and the importance of keeping their images secure. After this introduction, each child drew four images using Mikon which were checked by the teacher. If images are not suitable, children would be asked to draw another set of images. When then children's images were approved by teacher, the system generated distraction images that were used in each authentication attempt and then

the children received a notification email telling them that their account was complete. During the authentication phase, the children identified themselves by using their email address as their username following by the Mikon authentication, which consisted of four 4 x 4 grids which each contain one of the children's images and 15 distractor images. When a child chooses an image green circle would appear, but no indication of which image the child chose to avoid the choice being observed by others. Additionally, the login button at the end of the page is not activated until the child chooses an image from each grid. If a child fails to choose their own images, unlimited further attempts can be made, this was advised by the teacher to avoid suspension of children's account as some children could block others' account by trying to log in many times. One month after the children created the images, they were asked to login to the system and complete a homework assignment; this was repeated twice with two months gap between each login.

In term of memorability, the study showed that 87% of children successfully identified their images on the first attempt in all three logins. In term of predictability, the study found that Mikon did not work as expected, because all the children are from the same class and know each other, so they could predict what other children would like to draw. In addition, the children were in the same classroom doing the registration of their passcodes at the same time so the children could observe each other. However, when compared to the weak passwords that the children used before the study, Mikon performed better. In term of scalability, Renaud considered Mikon a more viable alternative to creating drawing than other systems, as there is no need to scan or upload images manually to the system.

Read and Cassidy (2012) investigated the types of passwords children choose. 26 younger participants (aged 6 and 7) and 23 older participants (aged 9 and 10) participated in a study with three stages: choosing a username; creating a password without any constraint on the length or characters; and recalling the password between 15 minutes to an hour later. The researchers found that younger participants created shorter passwords and usernames compared with older participants. Both younger and older participants created simple passwords. 13% of participants misspelled words accidentally or temporarily, so they may remember their password but not how to spell it. Some of the passwords created were guessable from the username the participant had chosen. The researchers concluded by suggesting replacing password authentication systems with other suitable authentication system if possible. They

proposed three design requirements for password authentication systems to be used by children:

- Password length: passwords should be not too long, between 4-8 characters especially for younger children.
- Password composition: complex password composition is part of password strength but this can make passwords difficult to remember for younger children. To balance between security and memorability, the alternative is to use password and question based prompts.
- Warning messages: for example, if a child misspells their password or creates a password similar to their username.

Lamichhane and Read (2017) used a game to study children's creation and understanding of usernames and passwords. In particular, they investigated whether children act like adults in using familiar and easy to guess usernames and passwords. In addition, they investigated if using a game would be appropriate to study password creation and recall. Participants were 17 children aged 7-8 in the UK. Each child has given a tablet on which they were asked a number of questions which might be reflected in their usernames and passwords (e.g., the name of their best friends and pet, their favourite colour), by a robot called Rewdon. Then they created a username and password. After one hour, they were asked to login to a system (which would provide them with information about what Rewdon had been doing) using the username and password they had created. The researchers used the data collected with the game robot and compared it with the chosen username and password to investigate their similarity. They found that 76% of participants chose a self-related username (e.g., contained the child's name). 53% created a self-related password. However, only 2 participants (11.7%) created a username and password that were closely related to each other. Most participants created simple usernames and passwords (e.g., one word with 1-3 digits with the word being something simple like a pet name). However, based on the information obtained from the children, 59% of usernames were judged hard to guess as were 71% of passwords. Like the children in the study by Read and Cassidy (2012), the children made spelling mistakes while creating usernames and passwords. 16 of the children managed to login after the hour, half at the first attempt, and the other half after asking the researcher for a hint. Reasons for not being able to log in included forgetting the username or password completely, making a spelling mistake, or making a mistake at the creation phase. In investigating the complexity of passwords, the researchers found the

participants struggled to remember more complex passwords. They concluded that children are not like adults in their ability to create and remember usernames and passwords, so they should be allowed to use passwords with a fewer number of characters, as well as having double entry of the password to mitigate against spelling mistakes.

Cole et al. (2017) compared graphical and textual passwords for children. The study included 13 participants aged between 6 to 12 years. All participants had previous experience with textual passwords; however, most did not have as many accounts as adults. In the graphical password condition participants created a username and chose an image then pointed to five places in the image to construct their password. Participants successfully logged in if they chose the correct image and found all five points in the image, if the point indicated was within 20 pixels of original one and in the same order. In the textual password condition participants chose a username and text password using the keyboard and were prompted to create a hint to help remember it. No information is given about any constraints on password length, composition etc.

The study was divided into two sessions with a within-participants design. Participants created passwords for five different accounts, presented to them randomly, some starting with graphical passwords while others started with textual passwords. After creating all the passwords, the participants logged into the accounts and then played a game for five minutes as a distractor task. They then attempted to login to their five accounts again, having five attempts on each account. Finally, they answered questions about the passwords such as "What was easier to remember?" "What did you prefer?" and "Which of these would protect you better?" In the second session (11 to 16 days after the first), only 10 of the original 13 participants returned. They were asked to login to the five accounts which were presented in the same order as in the first session when they had created their passwords. If for any reason a participant failed to login, the researchers provided the password (it is not clear how many attempts were allowed). At the end of this session participants were asked questions about which they thought was more secure, textual or graphical passwords; and whether they obtained any benefit from the password hint. Participants did very well on both authentication systems when logging in for the first time. However, their success rate dropped immediately after the game, more for text passwords than graphical ones. During the second session, participants did better with text passwords than with graphical passwords. The researchers concluded that graphical passwords are more memorable in the short term for children but more

difficult to remember in the longer term. In general, after two weeks even those participants who could not login could remember generalities of their password: the location, the image, the kind of username and password. The difficulties participants had with text passwords were capitalization, symbols, and spelling mistakes; and for graphical passwords, the accuracy of pointing location and order.

Hundlani et al. (2017) suggested the use of an authentication system for children which involves a parent, thus reducing the password burden for the child and giving the parent oversight of the child's account. The child only needs to click on log in and enter their username (in some cases parent could give the child the option to enter their password), then a request is sent to the parent who can allow or block this request. This is an interesting idea but does not add more information about children's own behaviour with authentication mechanisms, thus the paper will not be discussed further.

Maqsood et al. (2018) investigated children's password practices by giving children different rules in order to find out how they create passwords. 20 Canadian children participated, in the age range 11-13 years old. The researchers created three different websites with different complexity rules for the authentication that increase as a child moves from one to another. The first website is "QuizMe", on which participants need to create a password that contains six characters as a minimum. The second website is "FunZone", on which participants need to include the same rule as for QuizMe, but in addition have at least one uppercase letter, one lowercase letter, and one number. The third website is "OpinionMatters", on which participants need to include the rules for QuizMe and FunZone as well as one special character.

Participants were given a username to use on all three websites. On each website, participants created an account, followed by logging in, then completed a task (e.g., a quiz, poll, game), then moved on to the next website and repeated the process. Then they were interviewed about the websites and the password creation process (which was both useful and a distractor task). They were then asked to log in again to each of the three websites. The researchers found that the more complex the rules for passwords, the longer time it took the participants to create passwords. 40% of the participants had difficulties recalling their password during the first or second log in, however the researchers argued that this may could have been due to errors while entering the password originally. Additionally, 55% of participants used personal information to create their password. They reused or partially reused their passwords from one account to another, as adults often do. Participants tended to use uppercase characters, lowercase

characters and numbers in their passwords, even if they were not asked to do so. Nevertheless, 50% of participants found it difficult to understand the special character rule, mostly those aged between 11 and 12. Moreover, most participants were confident that the passwords they created were strong, in that they would be hard for a stranger to guess.

The researchers calculated password strength using Shannon's entropy formula (Shannon, 2001) and found no significant differences between the three conditions. They noted that entropy does not take into consideration dictionary attacks, common words, or patterns of characters. Therefore, they also used the NIST guidelines (NIST Special Publication 800-63B, 2017) to assess passwords on a scale from 1 (least secure) to 5 (highly secure). The NIST guidelines focus on the length and complexity of a password, its vulnerability to dictionary attack, the use of common words or character sequences. Two researchers scored each password in all conditions independently and most passwords scored between 1 to 3. This suggests that the participants were overconfident when they predicted the strength of their passwords. The researchers concluded, based on the two measures of password strength (entropy and an assessment using the NIST guidelines), that the passwords created were not strong. This shows that the young participants did not understand how to create a strong password.

Assal et al. (2018) evaluated the usability of a graphical password authentication system designed specifically for children called PassTiles. They compared similarities and differences between children and adults in terms of their preferences and performance with different versions of this system. Their study included 25 adult participants (20 of the adults were 18-30 years and the remaining 5 adults were over 30 years of age) and 25 younger participants (7-12 years) all of whom had experience of using authentication systems except one child. The adult study acted as a control condition for the child study.

(a) Objects PassTiles (b) Image PassTiles (c) Words PassTiles

Figure 3.1 The three versions of the PassTiles authentication system (Source: Assal, Imran and Chiasson, 2018)

All participants evaluated three versions of the PassTiles (object, image, and words, see Figure 2.1) although presentation for all schemes was in the same order, which may not have been the best choice. The password in each scheme consists of a sequence of five tiles to be chosen from a 6 x 8 grid of 48 tiles, with a counter at the bottom of the grid which showed the participant how many tiles remaining to be selected. All participants experienced the same four phases in the study. Phase 1 comprised signing consent form, the adult participants signed for themselves, the child participants had a parent sign for them. Then participants were given an introduction on how to use all three PassTile schemes. In Phase 2 participants memorized a system-assigned password for one scheme, they could practice entering it as much as they needed, then they logged in for the first time. Then they moved on to the next scheme and finally the process was repeated with the third scheme. At the memorising stage only, their password was highlighted in orange if they had not yet clicked on a tile, once they had clicked it would be highlighted in blue. At the login stage, no highlight was shown and after clicking five tiles a popup message appeared to inform the participant whether they have correctly entered the password or not. In Phase 3, an interview was conducted to measure participants' preferences and perception for the three different schemes. This phase also served as a distraction period and lasted 12 minutes. In Phase 4, each participant logged in for a second time with the three schemes presented in the same order as they had been for the first login. For each login participants were only allowed one attempt.

On memorisation time, there were no significant differences between the three schemes, although the adults took longer time memorising the Image scheme. The login time for both children and adults showed that the Word scheme was the hardest scheme to recall. Furthermore, the Image scheme was the easiest to recall for children at the first login and easiest

for adults at the second login. For login success, there were differences for children in either login for all three schemes. On the other hand, adults were significantly more successful logging in using the Object scheme on the second login. For degree of correctness, surprisingly, adult success rates were low compared to results from previous research. Unfortunately, there was no previous research related to PassTiles for children to compare to, but they also struggled with login. The reasons for the low success rates (for both adults and children) could relate to the study design, which involved having participants memorise three passwords in a short time and only allowing one login attempt. To address these issues, the researchers counted the number of correct tiles in each login attempt and they found both adults and children could easily correctly recall the Object scheme on the second attempt.

In the interview, participants were asked which scheme they preferred, which was the most difficult and which they thought safest. No significant differences were found between children and adults in their answers to any of these questions. However, the Object scheme was the most preferred and considered the least difficult by both children and adults. On the safety question, most of children were not familiar with security practices and could be vulnerable to attacks. In term of system design, both children and adults made the mistake of clicking tiles twice while they only needed a single click or the mistake of clicking on a tile again as they forget that they had already clicked it before. To avoid shoulder surfing, in the actual logins the clicked tiles were not highlighted Additionally, the youngest children (7 years old) found it difficult to pronounce the words in the word scheme making it difficult for them to remember their tiles. Both adults and older children in the Word and Object schemes tried to form a sentence from their password to help them remember their password. Adults in this study gave attention to pop-up messages that were designed to inform participants about whether their login was successful. However, the children did not. The researchers concluded that even if the majority of children learn about passwords from their parents or siblings, the coping strategies that adults use (and would try and teach their children) would not necessarily be appropriate for children. For example, formulating a sentence to remember a password is one of the methods the adults used, however in this study children struggled to use the Word scheme and took the longest login time with it. On the other hand, adults still struggle with passwords and do not always follow security best practices. Thus, children's cognitive level and preferences should be considered when designing authentication systems for them. The researchers' recommendations involve the use of training features to help children in the memorization phase, and that the system interface should be suitable for the children's age, for example using

colours and familiar objects. They also suggested combining the Word and Object schemes to improve memorability.

Chartofylaka and Delcroix (2018) evaluated children's understanding of best practices for selecting or creating a password and other online safety issues using a storytelling game activity called StoryPass. This study involved a class of 25 French children (10 – 11 years old). To make it easy for children to understand the concept of passwords, the researchers insured that they were involved from an early stage of password creation. The researchers first introduced the concept of passwords and usernames to the children by asking number of questions about their understanding of passwords, what they can unlock and what forms they can take. Next, as most of children stated that they created their passwords based on things that they are familiar with (e.g., their date of birth), they explained to the children how to make a password by mixing up words and transforming letters to numbers and special characters, following The French National Cybersecurity Agency (ANSSI) official recommendations that passwords should be a minimum of 12 characters with a mixture uppercase and lowercase letters, numbers, and special characters. Then, the children were asked to start to write a story. They were provided with an empty storyboard that had six cells and they were shown what should be the content of each cell, as shown in Figure 2.2. When creating their story 14 children completed the cells with text only, while 11 choose to use drawings. 23 children completed all six cells in the storyboard so the analysis was based on those who completed all cells. A sample of one of the children's storyboards is shown in Figure 2.3.

Figure 3.2 Storyboard template (Source: Chartofylaka & Delcroix, 2018)

Then the children were asked to choose two words from their storyboard and write them down. Finally, the children created their password from these two words by applying the strategies that they had learnt about good passwords.

Catman wanted to save all cats. His friends are catboys and his ennemis are doggils (waf!). They fight with each other. Doggils die and peace returns for all cats.

Password: **W@FDOG**

Figure 3.3 Sample of storyboard (Source: Chartofylaka & Delcroix, 2018)

Overall, 23 children (91%) successfully created their password and applied the good password strategies they had been shown. However, two of them used only one word instead of two words. Therefore, the researchers analysed the passwords of the 21 children who used two words. When creating their password, most of the children preferred to add special characters and numbers rather than an uppercase letter. Just over half of the children (52%) used at least three types of characters (uppercase letter, lowercase letter, number, or special character) and only one child used uppercase letters. The length of the passwords for most children (80%) was a minimum of 12 characters, which shows that the children had learnt the principles of good password composition which had been explained to them. The researchers concluded that it is good to involve children in password creation from the early stages. Children most likely will remember passwords that they create themselves, if it is combined with gaming activities. They thought that such type of StoryPass could be a new teaching method to be used with children to learn safe online behaviour and to understand important steps of password creation.

Ratakonda et al. (2019; see also Ratakonda, 2019) studied the level of children's understanding of authentication while creating and using usernames and passwords; they also studied the influence of adults (parents and teachers) on the children's understanding. These researchers conducted semi-structured online interviews with 22 children (aged 5-11 years) and 33 adults.

The sessions with the children consisted of:

- Creating an alphanumeric username and password with no restriction on length or type of characters included.

- Creating a pattern passcode using a basic Android-pattern mechanism (see Figure 2.4).
- Creating a numeric password using Android number passcode mechanism.
- The children were also interviewed about password composition, use of passwords in school, performance with passwords including reuse, and overall password preferences.
- In relation to children's password composition, security strength and whether passwords were self-related were measured.

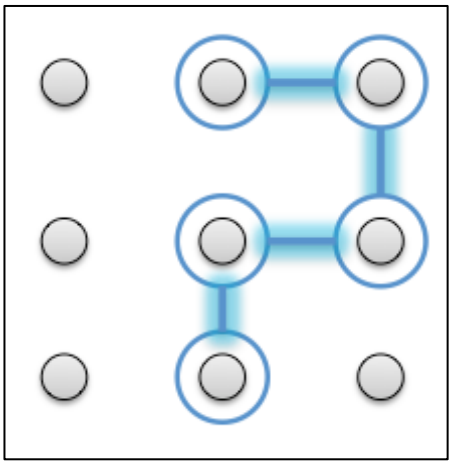


Figure 3.4 Sample of Android-pattern passcode (author's own drawing)

The interviews with the adults investigated their understanding of authentication, their own authentication practices, and their role in assisting children understanding and use authentications.

Strangely, the paper does not provide an analysis of the characteristics of the alphanumeric passwords that the children created (it only lists the characteristics such as length, composition components). From Table 2 in the paper, it can be calculated that the children created passwords with an average level of 7 characters, with a range from 4 to 14 characters. But 45.5% of the children created passwords of 5 characters or less and 10 created passwords that would be considered very weak in adult terms (e.g., the word "password", number sequences "1234" or their own name or initials). However, when asked about password composition, 54% of the children mentioned the need to include combinations of numbers, letters, and/or special characters and 14% mentioned the need to randomly arrange characters when creating

a good password. No information at all is provided about children's creation of the pattern passcodes or the numeric passwords.

In terms of the interview data, interesting results included the fact that just over half the children (54%) indicated that they use a "tool" (it is not clear what they meant by a tool, it appears to have included writing the password down) to save their usernames and passwords. In addition, nearly half the children (45%) reported being locked out of their accounts on occasion due to mis-entering a password incorrectly too many times.

The adults were asked how long it took for their child to enter their username and password. Approximately one third of adults (36%) indicated it would take 11-20 seconds. However, the researchers found that the children took more than 11-20 in the semi structured interview. In fact, this seems a very strange question to ask parents, who may never have thought about the time and it is a very short time to estimate accurately. It is not clear how the researchers measure the time and no precise statistics are given.

When one of the researchers asked the children to create their passwords, they did so in full view of the researcher, which is not good security practice. However, it could be that the children trusted the researchers, that they were making an exception, or that the children were not aware that others could be observing them. However, 68% of the children said that they would share their credentials with someone close to them. In relation to preference for password type, 82% of children preferred alphanumeric passwords compared to numeric or pattern passwords. 77%of the children reported using at least one application at school. The adults were asked about the role of teachers in helping children creating their credentials, 36% said teachers did help in this task. In relation to password reuse, 63% of the children indicated that they would not reuse their password in different applications. 77% of the adults stated that they play a role in the creation of children's password. Additionally, 68% of the adults indicate that they either create password for children or helping them in the creation process. This reflects the important role of adults in creating password for children.

Stewart et al. (2020) designed and evaluated two versions of a graphical authentication system called KidzPass for very young children and presented guidelines for designing graphical authentication mechanisms based on the two evaluations. However, there is some confusion about what age range is actually targeted in this research, apart from "very young" and "pre-

literate" children. The abstract refers to children aged 3 - 5 years. The evaluation of the first system with 8 children does not give the ages of the children, but in the discussion mentions that the system was targeted at children 4 - 5 years old. The evaluation of the second system was with 9 children aged 5 - 6. The guidelines developed from the work are targeted at graphical authentication systems for 4 - 6 year olds. However, by the age of 6 years, most children are no longer "pre-literate", they will have some basic literacy (Goswani, 2005). This does depend on the complexity of the language they are learning to read in and the educational system they are being educated in. Thus, the target age range and literacy of the children in this research does not overlap very much with the age range of the children in my research.

The first system developed and evaluated using familiar faces and the second using doodles created by the children. 8 children (ages not provided) participated in an evaluation of the first system. Parents provided a photo of a person familiar to the child, but not the person who fetched the child from school, so as to maximise memorability for the child but to avoid recognising photos from people relevant to other children in the school. In the first session, children registered in the system using images of animals which the children chose to be their dentification image instead of using a username such as an email address. The researchers argued that children of this age could not be expected to enter a text username. In addition, the children were shown how to choose their authentication image. Then in the authentication phase, the children had to choose their familiar face from a grid of 2 x 3 images of faces. The other faces were from other children's images in the evaluation. When they had successfully logged in the children go to play a game (time not specified) and answer questions about KidzPass. One week later, the children logged in again and again were allowed to play a game and answer questions about their experience with KidzPass. In terms of efficacy, the children could successfully recognise their identification and authentication images, and during the second session the researchers reported an increase in the children's confidence. In terms of efficiency, the researchers thought that time to log in is not a reliable indicator of efficiency as it depends on the placement of the target image in the grid the child will find. In terms of satisfaction (a point I used in my research by randomising the placement of the target doodle or object). In terms of satisfaction, the researchers noted that the children preferred the graphical password in comparison to the text passwords which they used at school.

9 children participated (ages 5-6; gender distribution not provided) in the evaluation of the second system. In this system children were asked to draw two doodles which were stored in the system. In the first session, before registration, the children watched a video that explained how the system worked. In the registration phase, they registered using an animal, as they did with the first system. In authentication phase, children needed to find their two doodles in a 2 x 3 grid (grid size being the same as in the first system, however the distractor images in this system were doodles drawn by the researchers). After logging in, the children played a game (time not specified). One week later, the children logged in again, played a game and then answered questions regarding their opinion on KidzPass. For this system the questions were asked only once in the second session due to time constraints. The researchers assessed the usability of this system using the same measures in first system: efficacy, efficiency, and satisfaction. In terms of efficacy, children could successfully recognise their registration and authentication images, and at the second session there was an increase in the children's confidence. In terms of efficiency, the researchers noted an improvement in the children's time to log in on the second session. In terms of the children's satisfaction, the researchers noted that most children preferred the graphical passwords in comparison to text passwords.

Renaud et al. (2021) designed an additional version of KidzPass and then evaluated all three versions it. Children aged 4-5 years used the familiar faces version; children aged 6-7 years used the doodles version; 44 children aged 8 – 10 years used a new object-based version. Children in the study thought they were playing a memory game, not an investigation of authentication systems. The study tested the children's ability to remember four different items from four different 3 x 3 grids, using a printed grid. At the beginning of the study, the class teacher asked the children to focus on the board and then she displayed four objects (animal, car, ship, building) for five seconds without any comment, then the teacher completed the lesson as planned. After one hour 15 minutes, the teacher gave each child four pages each containing four different 3 x 3 grids. The pages were arranged differently before giving them to the children to avoid having the same page for two children next to each other. Children were asked to choose the object in that they have seen before. One week later, the teacher distributed new four pages and asked children to choose the objects they remembered from the previous week. The second week's session was only conducted with children aged 9-10 years due to the COVID-19 pandemic and the school closing. The researchers found that children could identify cars, ships, and animals' objects but they have difficulties with building objects. The researchers argue that children of this age are not familiar of all types of buildings,

therefore, they could not label the buildings they had seen earlier, which made it difficult for them to identify them in the grid. They recommend other researchers to be more careful when choosing type of images to be used in graphical authentication systems. This issue was only raised in the third version while familiar faces and doodles were successful options.

Ratakonda et al. (2022) conducted further research on authentication systems for children with four formative studies with 8 children aged between 6 - 11 years. These studies were conducted to understand children's authentication practices with alphanumeric passwords and a graphical password designed by the researchers called KidsPic. As a result of the studies, the researchers enhanced KidsPic and evaluated it online with 40 children aged between 6 - 11 years.

The studies were conducted over four sessions with a one week gap between each session. The first three sessions took place in a lab and the last session was conducted online due to the COVID-19 pandemic. In the first session, the researchers asked the children to create usernames and passwords using an alphanumeric authentication mechanism with no password length restriction. The children created their username and password, played an online game for 15 minutes, and then entered their username and password (this constituted the first formative study). In the second session, children entered the username and password they had created in the first session and then created two new usernames and passwords. One password was created using an alphanumeric authentication mechanism, but on this occasion with password length restrictions (i.e., no less than 8 characters) (this constituted the second formative study). The second password was created using the graphical authentication system, KidsPic. The consisted of four sets of images each in a 4 x 4 grid and children should choose 4 images for their password (third formative study). Then the children played an online game for 15 minutes and the entered the two passwords created at the beginning of the session. In the third session, the children entered the two passwords they created in the previous session, and then watched an educational video explaining "how and why to create a strong username and password using the alphanumeric authentication mechanism" and then asked to create a new username and password using an alphanumeric authentication mechanism (fourth formative study). Children then played an online game for 15 minutes and finally re-entered their most recently created password.

The study found that for alphanumeric passwords (with or without length restriction) children made significantly more login attempts when entering their password one week later than after 15 minutes of distraction. Children were able to successfully log in with their KidsPic graphical

password after one week and with significantly fewer attempts than their alphanumeric password. For passwords created after the educational video, this appeared to have a minor impact, in that the children used more symbols in their passwords. However, the number of attempts to log in after 15 minutes was greater compared with the alphanumeric passwords created in first two formative studies.

Using the results from the formative studies and a design session with an intergenerational design team of children (aged 6-11 years) and adults, the researchers enhanced the KidsPic system on security and usability measures. For usability measures in terms of memorability, researchers asked children to make up a story while choosing images in KidsPic (a well known memory strategy). When applying this technique, researchers found that all the children successfully logged in from the first attempt after both period of time: 15 minutes and one week.

With regard to security issues, the researchers suggested increasing the graphical password strength by adding more images and six categories of images, each category containing 149 images. Suggested categories were animals, vehicles, nature, monuments, superheroes, and emojis. To make it easier for children to select images for their graphical password, rather than have them look at a very large number of images at the same time, the researchers suggested dividing images in each category into three tabs with each tab containing a 7 x 7 grid of images.

The researchers assessed the usability of this design by conducting a pilot study with eight children in two sessions. In the first session, the children created a username and graphical password, the password consisted of six images each from a different category. Then children played an online game for 15 minutes and then entered their username and password into the system. One week later, children again attempted to log in and the researchers asked them their opinion of the system. In the first session most of the children (6/8) could enter their credentials on their first attempt, while in the second session all the children entered their credentials accurately on their first attempt. Two issues were raised by the children. Firstly, it took a long time to search through the images due to the large number of images on each page. Secondly, they suggested adding a new category of images related to food. As a consequence, the number of images per category was reduced to 108 (6 x 6 in each grid) and a food category was added.

The usability and password design goals were evaluated with 40 children (aged 6-11 years, mean age: 8.5 years) in a further study involving two sessions. During the first session, the

researchers explained how to create an alphanumeric password, the length should be at least 7 characters and how to create a KidsPic graphical password of 7 images. Then each child was randomly assigned to a condition of creating an alphanumeric password then a KidsPic graphical password or vice versa. After registration of these two passwords, children played an online game for 15 minutes and then entered their two passwords. This session concluded by asking the children questions related to their experience with the two authentication mechanisms. One week later, children entered their two passwords (the order of using the two authentication mechanisms was randomised) and answered the same questions as in the first session. The researchers found that children had more successful logins with KidsPic compared with an alphanumeric password in both sessions. However, it took them longer to register and login with KidsPic than with an alphanumeric password.

Table 2.2 summarises the research papers presented in this section.

Table 3.2 Summary of the empirical research on graphical authentication systems for children

Research papers published before the design of Study 2 (Chapter 4) and Study 3 (Chapter 5)					
Citations	Aim of the Paper	Age Group	Authentication Method	Results	Role in Current Thesis Research (Design\Evaluation)
Mendori et al. (2002)	proposed an authentication interface based on icons.	Grade 1 (age not specified)	Graphical authentication system using object – recognition based	• Almost all participants memorized their password. • Many mistakes in input order were made. • The interface with 16 icons was the quickest to use compared with 8 and 64 icons.	• It is not clear from these two research papers the number of logins, number of icons in each password, and whether participants used all icons in the password at the same time or gradually. • Age of participants is not clear in either papers and number of participants in Mendori et al. (2005) is not specified. • Therefore, these papers were not used in designing and comparing with the Doodle and Object pass authentication systems (Studies 2 and 3).
Mendori et al. (2005)	Improved on Mendori et al. (2002) interface by changing the placement of buttons and making the icons bigger	Grade 2 (age not specified)	Graphical authentication system using object – recognition based	• The 12 buttons interface produced the most correct entries compared with 8 and 16 buttons interfaces. • The 8 buttons interface was the quickest to use.	
Renaud (2009a)	Assessed the viability of using children's own drawings (Mikon) as an authentication system	11-12 years	Graphical authentication system using doodles – recognition based	• Most of the children successfully identified their images on the first attempt.	• Since the study was conducted with one class of children, participants may have close friendships that make their doodles predictable. • The design of this authentication system helped in designing DoodlePass authentication system and comparing its effectiveness. • However, this research did not evaluate the system in term of efficiency or satisfaction

Citations	Aim of the Paper	Age Group	Authentication Method	Results	Role in Current Thesis Research (Design\Evaluation)
Read and Cassidy (2012)	Investigated the types of passwords children choose	6-7 years 9-10 years	Text passwords	• Younger participants created shorter passwords and usernames compared with older participants • Both younger and older participants created simple passwords • 13% of participants misspelled words accidentally or temporarily	• This study helped in comparing with Study 1 and the effectiveness of the Doodle and Object pass authentication systems
Lamichhane and Read (2017)	Used a game to study children's creation and understanding of usernames and passwords compared with adult	7-8 years	Text passwords	• Children differ from adults in their ability to create and remember usernames and passwords	• Used in comparing with Study 1.
Cole et al. (2017)	Compared graphical and textual passwords for children.	6-12 years	Graphical authentication system using PassPoints – recall based and text passwords	• Graphical passwords are more memorable in the short term but more difficult to remember in the longer term. • The difficulties participants had: o Text passwords: capitalization, symbols, and spelling mistakes o Graphical passwords: accuracy of pointing location and order	• Used in comparing with Study 1 and effectiveness of the Doodle and Object pass authentication systems. • Could not use it in designing the Doodle and Object pass as this type of graphical authentication system relies on recall rather than recognition.

Citations	Aim of the Paper	Age Group	Authentication Method	Results	Role in Current Thesis Research (Design\Evaluation)
Maqsood et al. (2018)	Investigated children's password practices	11-13 years	Text passwords	• 40% of participants had difficulties recalling their password • Over half the participants used personal information to create their password • Participants were overconfident when they predicted the strength of their passwords	• Used in comparing with Study 1. • Children created 3 different passwords with 3 different complexities at the same, so validity of the results could not be generalized or used completely to compare it with other studies in this thesis (i.e. registration and login time (efficiency and effectiveness). • No exact measures were provided for effectiveness or efficiency, only the significant differences between the 3 passwords. • Children's satisfaction was not measured for this system.

Assal et al. (2018)	Evaluated the usability of a graphical password authentication system and compare the preferences and performance with adults.	7-12 years	Graphical authentication systems using three versions: objects, images, and words – recognition based	• Word scheme was the hardest scheme to recall for both adults and children.
				• Image scheme was the easiest to recall for both adults and children.
				• Object scheme was the easiest to correctly recall for both adults and children.
				• Object scheme was the most preferred and considered the least difficult by both adults and children.
					• The methodology used to test PassTiles schemas is different from that used in the Doodle and Object pass authentication systems in the following aspects:
					  ○ Three different schemas evaluated at the same time.
					  ○ Each authentication key consists of 5 images.
					  ○ All authentication keys used in the three schemes are system generated.
					  ○ Children were allowed to memorise their authentication key at the beginning.
					• Only satisfaction and effectiveness of this system were compared to ObjectPass, values of efficiency were not clearly stated.

Citations	Aim of the Paper	Age Group	Authentication Method	Results	Role in Current Thesis Research (Design\Evaluation)
Chartofylaka and Delcroix (2018)	Evaluated children's understanding of best practices for selecting or creating passwords and other online safety issues	10-11 years	Text passwords	• Most children successfully created their password and applied the good password strategies that had been explained to them. • Over half the children used at least three types of characters (uppercase letter, lowercase letter, number, or special character). • The length of the passwords for most children was a minimum of 12 characters.	• Main focus is on teaching children how to create strong passwords, that is: long, and uses uppercase and lowercase letters, digits, and special characters, which is not recommended as security best practices for children. Therefore, not used in this thesis.
Ratakonda et al. (2019) and Ratakonda (2019)	Studied the level of children's understanding of authentication while creating and using usernames and passwords and; also studied the influence of adults (parents and teachers) on children's understanding	5-11 years	Graphical authentication system using pattern passcode and numeric passcode – recall based, and text passwords	• The paper does not provide an analysis of the characteristics of the text passwords. • No information is provided about children's creation of the pattern passcodes or the numeric passwords. • Most of the children preferred text passwords compared to numeric or pattern passwords. • 36% of parents said teachers did help children in creating their credentials. • 77% of the adults stated that they play a role in the creation of children's password.	• Used in comparing with Study 1.

Research papers published after the design of Study 2 (Chapter 4) and Study 3 (Chapter 5)					
Citations	**Aim of the Paper**	**Age Group**	**Authentication Method**	**Results**	**Role in Current Thesis Research (Design\Evaluation)**
Stewart et al. (2020)	Designed two versions of a graphical authentication system (KidzPass) for two different age groups.	Not given 5-6 years	Graphical authentication system using familiar faces and doodles – recognition based	• For familiar faces authentication system (target is 4-5 years old, ages of children in the study not given): o In term of efficacy, children could successfully recognise their identification and authentication images. o In term of efficiency, the researchers thought that time to log in is not a reliable indicator of efficiency as it depends on the placement of the target image in the grid the child will find. o In term of satisfaction, children preferred graphical password more to text passwords. • For doodles authentication system (5-6 years old): o In term of efficacy, children could successfully recognise their registration and authentication images. o In term to efficiency, the researchers noted improvement in the children's time in Session 2. • In term of satisfaction, most children preferred the doodle passwords more than the text passwords.	• For evaluation comparison: o The first system (faces) was for children 4-5 years group which is not included in either systems in this thesis. • The second system (doodle) evaluated with only 5-6 years age which are similar to grade 1 in the DoodlePass study however, no statistical analysis was conducted for either effectiveness and efficiency. Therefore, only satisfaction was compared with the DoodlePass authentication system.

Citations	Aim of the Paper	Age Group	Authentication Method	Results	Role in Current Thesis Research (Design\Evaluation)
Renaud et al. (2021)	Designed an additional version of KidzPass and then evaluated all three versions.	4-5 years 6-7 years 8-10 years	Graphical authentication system using familiar faces, doodles, and objects – recognition based	• For object authentication system (8-10 years old): o The researchers found that children could identify cars, ships, and animals' objects but they have difficulties with building objects. o Researchers recommend other researchers to be more careful when choosing type of images to be used in graphical authentication systems.	• Only a paper based design for the system and no statistical analysis conducted. Therefore, not used in comparing with the Doodle and Object pass authentication systems.
Ratakonda et al. (2022)	Conducted further research on authentication systems for children with four formative studies. These studies were conducted to understand children's authentication practices with text passwords and a graphical password designed by the researchers called KidsPic. As a result of the studies, the researchers enhanced KidsPic and evaluated it online.	6-11 years	Graphical authentication system using images – recognition based, and text passwords	• Children had more successful logins with KidsPic compared to text passwords. • Children took longer time to register and login with KidsPic than with text password.	• Used in comparing with ObjectPass authentication system. • No exact measures were provided for effectiveness or efficiency, only significant differences between the two systems.

3.4 Interview and questionnaire research on authentication systems for children

Read and Cassidy (2012) whose work who was reviewed above (see section 2.3), investigated children's level of understanding of passwords. They had 14 participants (7 and 8 years old) answer a simple questionnaire. The questionnaire asked about what makes a good password, why do people use a password, and how many passwords does the child have? The researchers found that the participants knew that passwords should be hard to guess but simple to remember. Their general understanding of passwords was that they are used to prevent access more than to allow access.

Coggins (2013) also studied what children know about passwords. He conducted a survey with 74 children aged 9 -11 years in three different schools in the USA. Participants were asked to give an example of a strong and an easy password and then asked to explain the benefit of using strong password in "real life". The example strong passwords were analysed according to a scoring rubric based on accepted good security practices. Only 14 passwords created were "very weak", while other passwords are distributed equally (20 examples each) between "strong", "medium" and "weak". Participants were found have some idea of how to create strong passwords, as they used at least six characters including a combination of letters and digits and took into account the use of random characters. In addition, they gave sensible explanations of why strong passwords need to be used in real life, with keywords such as "secure", "hack", and "do not want people in".

Lorenz et al (2018) conducted a large survey of children's cyber security in Estonia. Over 10,000 children from Grade 4 to 9 took part. Unfortunately, detailed analyses of children of different ages are not presented, which would have been possible with a sample of this size. Some of the interesting results include the fact that 97% of children have their own smartphone, that the children do not understand security terms such as "identity theft", and that 34% of children did not use a password or other lock on their digital devices.

Choong et al. (2019a & b) conducted a survey with 189 children in two schools in the USA: 88 children aged 8-12 years and 101 children aged 11-15 years. In relation what devices the children use, the most popular was gaming consoles, used by over 80% of the younger children, while cellphones were the most popular for the older children, used by 87%. Additionally,

students in both age groups used computing devices both at school and home. The children's use of technology changed as they get older with the use of cellphones increasing by 20% from younger to older children. In addition, the older children used devices for texting and social media more than the younger children.

In relation to their current password usage, the younger children had on average two passwords for devices at school and three passwords for devices at home. The figures for the older children were very similar, with on average two passwords for devices at school and four passwords for devices at home. Most of both groups used passwords for school computers (more than 90%) and for home computers (71-80%). In addition, authentication was used for email, social media, cellphones, and home computers, and this tended to increase with age. The extensive use of authentication by children in this age range across a wide range of devices and applications show that they the need more passwords to be created, used and remembered.

The younger children's knowledge about what makes a good password comes more from home than from school. The younger children reported learning more at home (71.59%) than in school (38.64%), whereas the older children learned almost equally about good password practices at home (76.24%) and at school (73.27%). The majority of children in both age groups know to keep their passwords private, to sign out after their use of a computer, not to share their password, and to change it regularly. The reasons given for changing passwords were "when someone find out my password" (reported by 94.55% of younger children and 72.5% of older children) and "when I forgot my passwords" (54.55% of younger children and 68.75% of older children). The one bad practice the children reported is reusing a password for all accounts (57.95% of younger children and 78.22% of older children). In relation to the reasons for using passwords, most responses for both groups were related to 'privacy' (40.48% of younger children, 38.02% of older children) followed by 'safety' (21.42% of younger children, 19.24% of older children) with 'hacking' having the lowest percentage (7.14% of younger children, 4.69% of older children). However, it was clear to the researchers that the children were confused between the password concepts of privacy, safety and protection. Many children reported that passwords would keep them "safe". The researchers suggest that the relationship between passwords and security is unclear to the children. The researchers did not advocate the idea of scaring children into using passwords to ensure good security practices. They note that most of resources in cyber security education for children are focused on cyber

bullying that could be part of the confusion. Therefore, they support the need for training for people who deliver this information for children including parents and teachers.

Children's perception of how easy it is to create and remember passwords was higher for the younger children than the older children; for example, 76.14% of the younger children thought it was easy to make a password, compared to 54.45% of the older children. Furthermore, more than 70% of both groups find it easy to use keyboard or a touchscreen to enter a password.

In relation to children creating their own passwords, the younger children reported greater involvement of parents (69.32% had passwords created for them by parents or help in creating passwords) compared to the older children, 86.14% of whom created their own passwords or had little help from parents. Almost all children in both age groups (more than 90%) reported memorizing their passwords. The younger children use external aids to remember their passwords more than the older children, although about a third of both age groups write their passwords down on paper.

The children were asked to create a new password for the researcher. The average password lengths were 7 characters for the younger children and 10 characters for the older children. Most of the passwords in both groups consist of lowercase letters, followed by numbers. The use of symbols or white spaces was rare. The researchers used zxcvbn.js to measure the strength of children's password. They found children in both age groups tended to make very weak passwords (56.94% of the younger children and 34.04% of the older children produce the lowest strength score). Although the percentages show some modest improvement in password among older children, the researchers suggest that the reasons behind such weak passwords is not that the children do not want to protect themselves online, but that they do not know how to create or form strong passwords. The researchers argue that children should not be encouraged to use easy passwords as this might tend them resist using more complicated password as adults.

Choong and colleagues continued with this line of work (Theofanos et al., 2021) by collecting data from more children and extending the age range to children from 8 - 18 years old. In this study, responses from 1505 children were analysed, 425 children US 3rd to 5th grade elementary school children; 357 children US 6th to 8th grade middle school children and 723 high school students.

In relation what devices the children use, when the researchers compared the three age groups, children in the oldest group used laptops the most, followed by middle age group and then the young age group. Based on age group, as children grow older, there is a decrease in using tablets, while an increase in using cell phones. The results also showed that as children grow older, they increasingly use social media, do their homework, and text on technology. On the other hand, playing games decreases as they age. Increases in technology use by older children provide an argument for the need for an authentication system for children. For example, more than 80% of the high and middle school children indicated that they use the same password for everything.

Regarding password understanding, most children indicated that they learn about passwords at home (72.35%) and a little over half learn at school (59.90%), while a small percentage of children learn from the internet (24.48%) and friends (12.28%). In relation to why passwords are needed, younger children most often reported "preventing or allowing access", interestingly this increased to 100% of middle school children and then decreased to only 61.52% of high school students. "Privacy" was the most important reason to both middle and high school students (52.16% and 71.07% respectively). The researchers argued that the older children associated "access" with "privacy", and that children in this age group frequently use technology for activities that are related to their identity such as social media or texting. They start exploring and becoming independent, which explains why privacy is an increasing concern. On the other hand, the young children were more general in their use of "privacy", as their access to applications (e.g., social media, email, or texting) is more frequently supervised by an adult. This may explain why they do not associate the use of these applications with expectations of privacy.

This study also found nearly 90% of the elementary school children have passwords created by their parents or get help from their parents in creating passwords, compared to only 15% of the high school students. As for remembering passwords over 80% of all age groups reported memorising their passwords, and less than half write them down (47.03% for elementary school children, 34.38% for middle school children and 35.09% for high school students). In general, the children reported that they have good password practices, they memorised their passwords, trying not to write them down, ensure privacy of their passwords, and sign out after finishing work on computers. Nevertheless, their passwords frequently contained personal information and as they grew up, they shared their passwords with friends, especially phone

passwords. In relation to password characteristics and strength, the younger children used simple passwords because they are still learning the alphabet and numbers. Passwords chosen by all age groups were weak but improved in the older age groups.

The researchers concluded in all three of these related studies (Choong et al., 2019a & b, Theofanos et al., 2021) found that children showed that they have good knowledge of passwords and authentication. However, the researchers argued that children need cybersecurity education to reinforce this theoretical knowledge and provide more understanding of security issues. In addition, the gap between children's knowledge and their actual behaviour needs to be bridged.

Table 2.3 summarises the research papers presented in this section.

Table 3.1 summary of the interview and questionnaire research on authentication systems for children

Citations	Aim of the Paper	Age Group	Method	Results	Role in Current Thesis Research (Design\evaluation)
Read and Cassidy (2012)	Investigated children's level of understanding of passwords.	7-8 years	Questionnaire	• found that participants knew that passwords should be hard to guess but simple to remember. • Participants' general understanding of passwords was that they are used to prevent access more than to allow access.	• Used in comparing with Studies 1, 2, and 3.
Coggins (2013)	Studied what children know about passwords.	9-11 years	Survey	• Participants were found have some idea of how to create strong passwords. • Participants also gave sensible explanations of why strong passwords need to be used in real life.	• Used in designing and comparing with Study 1.
Lorenz et al (2018)	Conducted a large survey of children's cyber security in Estonia	4-9 years	Survey	• Participants did not understand security terms such as "identity theft". • 34% of participants did not use a password or other lock on their digital devices.	• Used in comparing with Study 1.
Choong et al. (2019a & b)	Investigated children's level of understanding of passwords.	8-11 years 11-15 years	Survey	• Found that children showed that they have good knowledge of passwords and authentication. • Argued that children need cybersecurity education to reinforce theoretical knowledge and provide more understanding of security issues.	• Used in comparing with Study 1.
Theofanos et al. (2021)	Continued the work of Choong and colleagues by collecting data from more children and extending the age range of the children	8-18 years			

3.5 Research on guidelines and best practice for passwords for children

To create appropriate guidance for educators and parents about how to introduce password knowledge and practices to children, Prior & Renaud (2020) suggested three sets of age appropriate password best practices and terminology (see Table 2.4). First of all, they derived password best practices from official sources such as the US National Institute of Standards and Technology (NIST), the UK Centre for the Protection of National Infrastructure and the UK government. Then, they investigated what information is presented to children in children's books and online resources. They then worked with professionals and parents to rephrase the information to produce three age appropriate password best practices and terminologies. The first level was designed for children aged 4 - 5 years and has three principles: "password issues", "password creation", and "password entry". The second level was designed for children aged 6 - 7 years and has six principles, including the three principles from the first level but with more details and explanation in "password issues". The third level was designed for children aged 8 - 9 years. This level has the same principles as in the second level but more details in some of the principles. No evaluation of the effectiveness of these principles is presented in the paper.

Table 1.2 Password best practice for children of different ages (Prior & Renaud, 2020)

Age 4 - 5	Age 6 - 7	Age 8 - 9
Password Issues (e.g., You might not be able to play a game if you forget your password)	Password Issues*	Password Issues*
Password Creation (e.g., always ask your teacher, mummy, or daddy if you are not sure about anything)	Password Creation (e.g., Make up a silly sentence)**	Password Creation*
Password Entry (e.g., Before you enter your password have a quick look that no one is peeking)	Password Entry*	Password Entry*
-	Why Password? (e.g., Stopping others from getting into your computer)	Why Password?*

-	Password Leakage Consequences (e.g., Someone telling the computer that they are you)	Password Leakage Consequences (e.g., Someone pretending to be you)**
-	Password Retention (e.g., Remember your password)	Password Retention*

* Example for this practice is the same as for younger age, not repeat it.
** Example for this practice is different in wording or meaning than for younger age.

Stewart et al. (2020), whose research was discussed above (see section 2.3), proposed set of guidelines for designing graphical authentication systems for pre-literate children (as noted above, the precise age range is unclear). The guidelines are summarized in Table 2.5. The guidelines are a strange mixture and not clearly expressed as guidelines. Given these guidelines are aimed at systems for pre-literate children, it seems strange to start with "use icons as well as text". Earlier in the paper, the authors themselves argue for the "use of pictures INSTEAD of text" (emphasis added). Research on graphical authentication for children had started with the work by Mendori et al. (2002, 2005) based on the assumption that young children have difficulty with text, so this guideline should be "use pictures instead of text". In addition, two of the guidelines are referring to the same issue: "Identification image choice" and "authentication image type must be chosen carefully" both refer to choosing a class of image that is familiar and of interest to the target audience of children. Again, Mendori et al. (2002, 2005) had already addressed this issue, pre-testing images to ensure that children were familiar with them and could distinguish between particular instances. In addition, citing Paivio and Csapo (1973) to support the use of images versus text is very odd, as the guidelines are aimed at systems for pre-literate children, so they do not yet have memory for words, so the claim that "this also confirms the superiority of picture memory, even in very young children" makes no sense.

"Delivery method matters" is not about the design of authentication systems for children, but about the ergonomics of designing any digital system for children. There is a considerable research literature on this issue and the use of tablets in particular by very young children, which could be drawn on for this guideline (Bruckman et al., 2012; Markopoulos et al., 2021), which does not mention other possible devices (e.g., smartphones with smaller screens, computers with keyboard-mouse interaction etc).

"User testing is critical", "incentives matter", "recruitment", "limitations (small sample)" and "limitations (time consuming)" again are not about the design of authentication systems for

children, but apply to all research with children, particularly about in relation to technology (Bruckman et al., 2012; Markopoulos et al., 2021; Skapyak, 2023).

It is also strange that the authors do not draw more on previous research on authentication for children to emphasise points such as using recognition rather than recall, not placing excessive cognitive and memory burden on children, children different abilities to draw, not discussing the challenges of using tabs in the authentication interface with children, and authentication key actual characteristic is to have more than one image.

Table 1.3 Guidelines for designing graphical authentication mechanisms for pre-literate children (Stewart et al., 2020)

1	Use icons as well as text	The use of text on the login screen should be avoided.
2	User testing is critical	User testing with the intended user population is the other way to determine if the designed system is suitable.
3	Identification Image choice	The researcher also noted that the animal identification images were very popular. Allow the children to select their "favourite" animal created a connection between the child and their username image and since most of the children were able to recall their animal image without assistance, this also confirms the superiority of picture memory, even in very young children (Paivio and Csapo, 1973).
4	Authentication Image type must be chosen carefully	The image type chosen for the graphical password is key to the success of the application. Using pictures of familiar adults was very successful in the first study as it didn't require the children to memorise a specific image. The immediately recognised their familiar face and were able to associated that face with logging into KidzPass, even when it was surrounded by other faces. The children quick realised that each picture was different and knew that one was "theirs". The doodles were equally memorable in the second study, proving a reasonable replacement for familiar face images.
5	Randomisation of image choice	The faces shown in the first study's challenge set were randomly chosen. Children could swipe through the sets until "their" face appeared. Some of them became frustrated when they had to swipe through a number of successive challenge sets. Hence, the next version of KidzPass implemented a maximum number of challenge sets to swipe through before the child's doodles appeared. This change worked well.

6	Incentives matter	User incentives are important in providing a desire for the young children to want to engage with the system. This applies to the stickers the children were rewarded with after using KidzPass. The good feeling was paired with the success of logging in and the gratification of getting to play the game. This meant the children were excited to use the system in the follow up session and enjoyed the process.
7	Delivery Method Matters	Using a tablet for user testing proved a good choice. There was one incident in the first study where a child accidentally selected an image while attempting to scroll downwards. This was most likely due to the learning curve that comes with using a tablet computer and depends on the size of the tablet screen. The researcher found that with a smaller, slower tablet (Nexus 7), there was a higher risk of this happening.
8	Recruitment	We had some difficulty recruiting children. In the first study, we realised that this was because we were asking parents to do more than sign a consent form. We were asking them to provide us with a photo of someone familiar to the child. We had provided them with complete instructions for what the phot should look like. In retrospect, we created a barrier to participation in very busy parents' lives. For the second version of KidzPass we switched to asking the children themselves to draw images for us … Parents were then happy to permit their children to participate in the case. Yet, these kinds of studies have stringent ethical requirements and we still found it difficult to recruit children. Many schools in our geographical area receive multiple requests to participate in University studies. This has led them to limit the number of requests they acquiesce to.
9	Limitations: Small sample size	The small sample size is a limitation in both studies, in terms of carrying out quantitative analyses.
10	Limitations: Time consuming	The evaluation was also very time consuming because of the age of the participants. For these initial studies, we wanted to hear their voices and not rush them, but rather give them time to express their opinions.

Renaud et al. (2021) extended the work of Stewart et al. (2020) and proposed principles for designing and evaluating authentication systems suitable for children from ethical and technical perspectives. These principles were based on their review of a number of sources: the "Age Appropriate Design Standard" published by the UK Information Commissioner's Office (2020); guidelines summarised from reviewed research literature; lessons learned from evaluating their system "KidzPass"; and properties that help image memorability. The ethical principles were:

- Children's best interest: Design the mechanism in line with the child's capabilities.
- Data protection impact assessment: Develop a Data Protection Impact Assessment (DPIA).
- Age appropriate application: User incentives are important in providing a desire for the young children to want to engage with the system. Reward the children for using KidzPass by letting them play a game.
- Transparency: researchers should inform children at the beginning of a study that they have the right to withdraw at any time.
- Detrimental data use: Do not use the child's data for any other purpose than authentication.
- Policies and community standards: Within the EU, ensure that GDPR standards are adhered to. Only collect data that is necessary as part of the authentication and make sure all child-provided data is stored either encrypted or hashed in order to ensure that no sensitive information the child potentially entered can leak in plaintext.
- Data minimization: Do not collect any information that is not strictly required to authenticate the child.
- Data sharing: A child's data can only be shared with explicit consent from the parents.
- Nudge techniques: Nudges must be used only be used for the good of the child, not for the good of the platform.
- Online tools: Ensure that the child's GDPR rights are upheld, and that parents can satisfy themselves of this by including a link to terms and conditions and a contact email address in the interface. (i.e., ensure children know their rights in collected data before they participate).

The technical principles proposed were:

- Use a tablet: This ensures that children unfamiliar with a mouse can devote all the cognitive bandwidth to using the mechanism.
- Use age appropriate images, targets and distractors: For the youngest children, maximise memorability and ease of use by using familiar images. For older children, generic images can indeed be used, but only when chosen with care. Ensure that the images you choose can be labelled uniquely by the target user group i.e., that the vocabulary and categorisation can be carried out by an average child of that age.
- Use age appropriate literacy requirements: Children in the 4-5 age group should not be required to identify themselves by entering a textual identifier such as an email address. Allowing children to choose 'their' image will work better. Older children may well be able to enter emails with ease.
- Recruitment: Work with educational authorities to recruit children, or run cyber awareness events and evaluate new mechanisms as part of the event activities.
- Hear children's voices: It is important to hear the children's voices, respecting their opinions and perceptions of the authentication mechanisms we design for them.
- There are no shortcuts: Evaluations of these mechanisms with children are going to take much longer than evaluations with adults. Expect that and do not try to speed things up.
- Use free software: This ensures that any adopter can use it because financial limitations do not deter usage.

This is a very diverse set of principles which mixes design principles with general points about conducting evaluations with children. The researchers have derived them from their own research, but there is no evaluation of them by independent developers or researchers.

3.6 Conclusions

This chapter reviewed the research on children's use and understanding of passwords, conducted via both empirical and survey methods. It also reviewed research on the guidelines for best practice for authentication systems for children. The key points which emerged from the research which particularly guided my programme of research are highlighted here.

Children aged 6-12 years still struggle with language and made spelling mistakes (Cole et al., 2017; Lamichhane & Read, 2017; Read & Cassidy, 2012; Stewart et al., 2020). Although it is

assumed that the children who participated in the studies reviewed in this chapter were native speakers of the languages being used in the password systems, they are not necessarily confident in their spelling yet. However, in many countries where the language does not use the Latin alphabet (e.g., Arabic speaking countries), passwords must still be created using this alphabet. So this is very likely to create additional problems for children, but this issue has not yet been investigated.

Much of research review supports the conclusion drawn by Assal et al., (2018), that young children generally have a good knowledge about password creation and management, however, in practice they do not necessarily apply this knowledge. For example, children know that a password should include a large number of characters but the number of characters that they actually use when creating a password is low. This is probably due to the cognitive and linguistic abilities of the children at this age.

Another important problem for children is remembering text passwords, investigated by a number of researchers (Kumar et al., 2017; Lamichhane & Read, 2017; Maqsood et al., 2018; Ratakonda et al., 2019; Ratakonda et al., 2022; Read & Cassidy, 2012). This strongly suggests that authentication systems based on recognition of items rather than recall of passwords is more appropriate for children. Such systems using doodles and images have been investigated in a number of studies (Assal et al., 2018; Cole et al., 2017; Mendori et al., 2002, 2005; Ratakonda et al., 2022; Renaud, 2009a; Renaud et al., 2021; Stewart et al., 2020). However, apart from the early Japanese work (Mendori et al., 2002, 2005) most of the research has been conducted in the English speaking world (particularly the USA, Canada and the UK). One study was conducted in France (Chartofylakas & Delcrois, 2018), one study was conducted in Estonia (Lorenz et al., 2018), although it collected little information about password knowledge and use, and one study may have been conducted in South Africa (Stewart et al., 2020), it is not clear. Thus, very little of the research on authentication systems for children has been conducted beyond the English speakers and users of the Latin alphabet. No research could be found which has been conducted in Arabic speaking countries, which raises particular issues for password creation and use.

The research reviewed often has methodological problems. Many of the studies reviewed used small sample sizes which limits the generalisability of their results. However, conducting research with children is time consuming and gaining access to samples of children requires considerable ethical approval, so the small samples are not surprising. The research often deals

with children only in a narrow age band and does not always consider the cognitive developmental changes that children go through, particularly in elementary school years (6 – 12 years). Studies which do include a wider age range often do not analyse for differences between children of different ages or cognitive stages.

One more important issue in the research reviewed is ecological validity. Some of the work reported that creating different authentication key at the same time to evaluate it has some effect on the results as this does not reflect how do children deal with their authentication key on a daily basis (Maqsood et al., 2018; Assal et al., 2018). However, it is not clear from this literature what the usability effect is of having the same type of graphical authentication key for different accounts (i.e. doodles, objects, or images).

Therefore, it is important to further investigate the area of usable authentication systems for children, taking into account children's mental abilities and cognitive development, and their native language.

Chapter 3

Study 1: Exploratory Study of Children's Understanding of Online Security and Passwords

4.1 Introduction

Exploring children's understanding of security and best practices was an important step to initiate my research and help me develop ideas for better authentication systems that can serve new generations of children, taking into account their levels of cognitive ability and memory development that are form different of adults. The literature review (Chapter 2) showed that children struggle with text passwords as a result of spelling mistakes and their lack of ability to memorise and recall them. Given that most of the previous studies of children's understanding of passwords have used English native speakers, this is not sufficient to understand the situation worldwide. As elaborate later in this chapter (section 3.4.3), children who are native speakers of Arabic have problems in using passwords that are written in the Latin alphabet. The Arabic language is the fourth most commonly spoken language in the world, with 362 million native speakers (Lane, 2023). Therefore, it is important to understand the extent of Arabic children's knowledge regarding security aspects and best practices. So, in this first study for my PhD programme of research, I explored children's knowledge about passwords and security with Arabic speaking children from the Kingdom of Saudi Arabia (KSA).

It addressed the following research questions:

RQ1: Do Saudi children use digital devices at home or at school?

RQ2: Do Saudi children understand the reasons for having passwords and how to create good ones?

RQ3: Do Saudi children have linguistic problems in relation to password creation in the Latin alphabet and in English?

RQ4: At what age do Saudi parents think it is important for their children to understand how to make passwords for online systems?

4.2 Method

4.2.1 Design

The study used semi-structured interviews with Saudi children aged 6 to 12 years and one of their parents. Some of questions used were derived from Coggins (2013). The interview comprised closed and open-ended questions and was divided into three sections: demographic questions, questions for the parent, and questions for the child. Questions for the parent covered their knowledge of their child's use of digital devices and passwords, their child knowledge of English, and their opinion about the importance of educating their child about passwords. Questions for the child covered their use of digital devices and passwords, their level of understanding of the need for passwords, and their ability to create and explain weak and strong passwords.

The reason behind specifying part of questions for parents was that I thought they would be able to give more accurate answers to these questions. The interview was conducted face to face and other researchers participate in conducting interviews to increase the number of participants (see section 3.2.4 for more details). Both qualitative and quantitative analysis of the data were undertaken.

In relation to the data analysis, having a sample of children in the study from 6 to 12 years, and trying to analyse their data according to Piaget's development stages mentioned in the literature review chapter (Chapter 2, section 2.2) was not possible. This is because most of the children will be at the concrete operational stage, with a few children probably at the preoperational and formal operational stages. However, without testing the children individually to understand which stage they were at, it would have been unwise to make assumptions – for example that children in Grade 1 are preoperational, children in Grades 2 – 5 are concrete operational, and children in Grade 6 are formal operational. Piaget noted that children reach each of these stages at different times, and the ages are only a guide. Thus, analysis was conducted a number of

ways: each grade/age group, each pair of grade/age groups, or lower and upper classes; and in some situations more than one way (see section 3.2.5).

4.2.2 Participants

39 children participated, aged between 6 and 12 years. This included 21 (53.9%) girls and 18 (46.2%) boys. All children were volunteers from different schools in Saudi Arabia and Arabic is their first language (see Table 3.1). Approximately half the participants were studying in privately-funded schools, and approximately half (19/39, 48.7%) were studying in state-funded schools. In Saudi Arabia children in state-funded schools start studying English in Grade 4[2] (approximately 9 -10 years of age). Children in privately-funded schools start studying English in Grade 1 (approximately 6 - 7 years of age) and have a more intensive English curriculum. Thus, children in privately-funded schools will have more proficiency with the Latin alphabet and English words (see Appendix A.4 for more details regarding the difference between state-funded and privately-funded schools in Saudi Arabia in term of English and Computer curricula).

All the parents were mothers, and no further demographic information was collected about them.

Table 4.1 Gender and school grade/age breakdown of the children interviewed in Study 1

Grade	Gender		School Type		Total Number of Children
	Girls	Boys	Privately-Funded School	State-Funded School	
1 (6-7 years)	5	2	4	3	7
2 (7-8 years)	4	2	3	3	6
3 (8-9 years)	2	5	4	3	7
4 (9-10 years)	3	4	4	3	7
5 (10-11 years)	3	3	3	3	6
6 (11-12 years)	4	2	2	4	6
Overall	21 (53.9%)	18 (46.2%)	20 (51.3%)	19 (48.7%)	39

[2] In 2021, in Saudi Arabia children in state-funded schools started to study English starting from Grade 1, however, this change did not have an effect on my participants as data collection done before that time.

4.2.3 Interview schedule

The semi-structured interview schedule consisted of 30 closed and open-ended questions. The schedule consisted of three parts: demographic questions, questions for the parent and questions for the child. An electronic version of the interview was created in the Qualtrics survey tool; this allowed all the interviewers (see section 3.2.4) to enter the answers to interview questions directly using the Qualtrics survey tool, for ease of access and later analysis. The demographic questions asked for the parent's email, their child's age and grade, gender, and type of school.

Questions for the parents: 16 questions were asked to the parents. Questions in this section asked about the type of devices used by the child at home or school, the child's use of devices and applications, whether the child has passwords to access these devices or applications, the structure of their passwords, the child's experience in resetting their passwords, the child's ability to use the Internet, whether the parent uses or creates the child's password, the child's knowledge of English, and their opinion of the importance of educating their child about best password practices.

Questions for the children: 7 questions specifically for the children asked about the purpose of passwords, number of passwords they have, and their understanding of weak and strong passwords. To make this question more concrete for them, they were asked to create a "easy" password and a "strong" password, and then asked to explain why they were easy or strong. (See Appendix A.2 for the full interview schedule).

Initially a pilot study was conducted on a preliminary version of the interview schedule with six children from different grades and schools and their parents. The pilot interview was conducted online with five children using the Skype or FaceTime video applications, while one pilot interview was conducted face-to-face. This highlighted a number of areas for improvement. For example, the question (Why do you think that strong computer (or website) passwords are used in real life?) was edited to (Why do you think that strong passwords are used in real life?). As a result, I rewrote or deleted some questions and added other questions (see Appendix A.1 for a table with the changes and improvements to the interview schedule).

The mapping of the interview questions to the research questions of the study is summarized in Table 3.2

Table 4.2 Mapping interview questions to the research questions in Study 1

Research Question	Interview Question	Question for Parent / Child
RQ1: Do children use digital devices at home or at school?	8. What digital devices does your child use at home?	Parent But children contributed to answers
	9. What does your child use these for?	Parent But children contributed to answers
	14. Does your child have any accounts on the Internet/Web themselves?	Parent
	16. What digital devices does your child use at school (you may need to check with them)?	Parent But children contributed to answers
	10. Do any of the digital devices your child uses at home need a password/passcode to open?	Parent But children contributed to answers
	15. Do any of these accounts need passwords?	Parent But children contributed to answers
	17. Do any of the digital devices your child uses at school need a password/passcode to open?	Parent But children contributed to answers

Research Question	Interview Question	Question for Parent / Child
RQ2: Do children understand the reasons behind having passwords and how to create good ones?	25. Why do people have passwords?	Child
	12. Has your child ever had to change a password at home?	Parent
	19. Has your child ever had to change a password at school?	Parent But children contributed to answers
	24. About how many passwords do you have?	Child
	26. Why do you think that strong passwords are used in real life?	Child
	28. Can you give an example in each box below of a computer (or website) password that would be very easy to guess and example of a strong (hard to guess) password? (Please do not use your own password)	Child
	29. Why was that an easy password?	Child
	30. Why was that a strong/hard password?	Child
	27. In your opinion, what makes a good password?	Child
	13. Does your child use the Internet/the Web by themselves?	Parent
	20. Do you login with passwords to systems that your child uses?	Parent
	21. Do you create passwords for your child to use for online systems?	Parent

Research Question	Interview Question	Question for Parent / Child
RQ3: Do Arab children have linguistic problems in relation to password creation in Latin alphabet and in English?	22. How many English words does your child know?	Parent
RQ4: At what age do parents think it is important for their children to understand how to make passwords for online systems?	23. Do you think it is important for your child to understand about making passwords for online systems at their age?	Parent

4.2.4 Procedure

The study was approved by the Physical Sciences Ethics Committee of the University of York. Following that, an initial consent between myself and the parent was collected via text message. At the beginning of the interview, the parent signed a consent form which was uploaded in advance to the Qualtrics survey tool and they asked their child if they wanted to participate in the presence of the researcher. Additionally, the children's verbal assent to participate in the research was sought. They also have been told that they have the right to withdraw from the study any time.

All interviews were conducted face-to-face except one interview which was conducted online using the FaceTime video application. The interviews took place at the participant's home in a quiet room with the parent and the child. All data were recorded by the interviewer using Qualtrics survey tool to facilitate analysis.

The researcher interviewed 13 child/parent pairs, while 26 were interviewed by 11 colleagues of the researcher. All the colleagues have a degree either in computer science, information technology, or information system (Bachelor, Master, or PhD). This is was to increase the number of children interviewed and to have as many face-to-face interviews with children and their parents as possible. Therefore, two general questions were added to the Qualtrics questionnaire which allowed the interviewer to identify who conducted the interview and their profession. To ensure accuracy in data collection, I briefed the interviewers in detail about the interview purpose and process before they conducted any interviews (see Appendix A.3 for a table with the interviewer demographic information).

At the beginning of the interview, the researcher explained to the parent the aims of the interview. The parent was told that the interview would contain two groups of questions. One group should be answered by the parent themselves and in some cases children might add to their parent's answers, if the parent did not know or was not sure of the answer. The other group of questions should be answered by the child. The parent was also informed that in the questions for the child there are no correct or wrong answers, so the child should try to answer them themselves. The researcher also assured the parent that the child would not be asked to reveal any sensitive information related to the child's passwords or passwords used at home.

The child was told that the researcher needed their help by answering some questions, and they were usually excited to do so. For example, in the password creation question (Q28. Can you give an example in each box below of a computer (or website) password that would be very easy to guess and example of a strong (hard to guess) password?) children were told: “I have homework for my PhD and my supervisor asked me to get assistance from children to create two type of passwords, easy and hard, could you please help me! But be careful do not reveal your password to me we will create a new one”.

Overall, for ethical aspects, I tried first with small number of children to explain my actual work and the meaning of research, however, the children did not understand. The reason I think is that in Saudi Arabia children at elementary and the beginning of middle school (Grade 1-7) do not use the term research and instead homework. In addition, previous research in the literature review chapter (Chapter 2) provides little guidance on how to explain research studies to young children.

4.2.5 Data preparation

Data on a number of the quantitative variables from the study were not normally distributed, so non-parametric statistics were used.

In a number of questions, the effects of the children’s age/grade were investigated. However, in some instances the number of children in each grade was small, so the children were grouped into three levels of two grades (Grade 1 & 2, Grade 3 & 4, and Grade 5 & 6).

To analyse responses to the open-ended questions a mix between deductive and latent approach used and a Codebook thematic analysis was used (Alhojailan, 2012). These were: Q25. Why do people have passwords? Q26. Why do you think that strong passwords are used in real life? Q29. Why was that an easy password? Q30. Why was that a strong/ hard password?

The thematic analysis was conducted in a number of steps. First, my supervisor and I met and discussed an initial framework for the codes. Second, I conducted all the coding using these initial codes. Then I gave this initial coding to my supervisor to check and refine it for a new version. Third, together we developed new codes for the participants’ answers in two different version and then compare and agree on a final version. For Q29 and Q30, in some cases the

children's answers were analysed according to the actual answer they gave and sometimes according to the password that child created in Q28 as an example of an easy or hard password, whichever provided the more detailed information. This was because children did not always know how to express the meaning of things in their password, but the meaning could be understood from the password itself. For example, one child (P8, G4) wrote his easy password for Q28 "موية"which means water in English. However, when he answered Q29 he said "*I do not know it is easy word*".

4.3 Results

4.3.1 RQ1: Do Saudi children use digital devices at home or at school?

To investigate RQ1, the answer to the questions in the interview that are related to: type of digital device that they use, the activities the children reported undertaking with their digital devices, and the use of password for digital devices or online accounts, are analysed. As mentioned in the Procedure (see section 3.2.4) questions on these topics were directed at parents, but the children might also contribute to answer the questions.

4.3.1.1 Digital devices that children use.

Parents were asked the types of devices that their child uses and their use at both home and school.

Table 3.3 shows the different types of digital devices the children use at home and at school, all children (39/39, 100%) use digital devices at home, while about half (22/39, 56.4%) use them at school. At home (Q8) all the children use digital devices; most of them use tablet computers (71.8%), about half use mobile phones (53.8%) and games consoles (48.7%), after that laptop computers (38.5%), and least frequently desktop computers (7.7%). One child mentioned a smart TV.

At school, about half the children (22, 56.4%) use digital devices. Nearly all those children indicated that they use desktop computers (95.5%) at school, while only a few use tablet computers (13.6%).

Table 4.3 Use of different types of digital devices at home and at school

Digital devices	At Home N=39	At School N=22
Tablet	28 (71.8%)	3 (13.6%)
Mobile phone	21 (53.8%)	0 (0.0%)
Game console	19 (48.7%)	0 (0.0%)
Laptop	15 (38.5%)	0 (0.0%)
Desktop	3 (7.7%)	21 (95.5%)
Other	1 (2.6%)	0 (0.0%)
None	0 (0.0%)	17 (43.6%)

Table 3.4 shows the activities the children reported undertaking with their digital devices at home. The options that are listed in the interview to choose from are: Games (i.e., video games), entertainment (i.e., watching YouTube), web (i.e., searching for information), school (i.e., accessing school blackboard), texting (i.e., sending messages through online application), social media (i.e., Instagram), Email, homework (i.e., online homework in Classera platform an online teaching platform, widely used in Saudi Arabia and other countries, https://me.classera.com/). The most popular being playing games (reported by all the children), entertainment (87.9%), about half use social media and school (43.6%) and only a small number of children use it to check their email (7.7%).

Table 4.4 Activities with digital devices at home (N=39)

Activity	Number of Children
Games	39 (100%)
Entertainment	34 (87.2%)
Social media	17 (43.6%)
School	17 (43.6%)
Web	14 (35.9%)
Homework	14 (35.9%)
Texting	11 (28.2%)
Email	3 (7.7%)

4.3.1.2 Digital devices and the use of passwords

The digital devices children use at home generally have a password (reported by 34/39 children, 87.2%). Interestingly, more children indicated that their home devices have passwords than reported having passwords themselves (only 29 children indicated this, see section 3.3.2.2). This may mean that they do not know the password for their device themselves, that it is entered by a parent.

The children who use digital devices at school were also asked about their use of passwords for devices at school. Only a minority (4/22, 18.2%) have passwords for their school devices.

Regarding using passwords for online accounts, about half the children (18/39, 46.2%) have online accounts and most of those children (16/18, 88.9%) have passwords for these accounts.

4.3.2 RQ2: Do Saudi children understand the reasons for having passwords?

4.3.2.1 What children thought about password usage

To investigate children's understanding of why people need passwords, a thematic analysis was conducted of their answers to the open-ended question on this topic (Q25. Why do people have passwords?). Two children did not answer this question, so the analysis is based on answers from 37 children.

Table 3.5 summarizes the results of the thematic analysis. The main themes which emerged were:

- **What**: is protected by a password.
- **Other's actions**: what actions are others taking that requires the child to have a password.
- **Who:** is a password protecting your device/information from.
- **Child's actions**: What action is the child taking with a password.

Most children's comments mentioned one or more "What" and "Other's Actions". In term of "What" is being protected by a password, most common categories were hardware (e.g., devices, iPads, computers, mentioned by over half the children (62.5%) and software (e.g., files, programs, also mentioned by approximately one third of the children (29.7%). The children also mentioned actions by others which a password might protect against; the most frequently mentioned action (mentioned by 83.8% of children), was that the child thought that another person can gain access to their device or information, followed by to destroy something (10.8%). In terms of who those others are, the "Who" main theme was mentioned by most participants, with the frequent response being "people in general" (78.4%); other less frequent responses included other children, the child, their siblings, and strangers. Finally actions the child was taking by having a password was only mentioned by a small percentage of the children. Reasons for actions included to prevent access (10.8%), to secure or protect (5.4%).

It is interesting to note that about a third of the children (10/37, 27%) used security words in their answers (e.g., privacy, hack); most of the children who used these words are in upper classes of elementary school, Grades 4, 5, and 6 (8/10, 80%) (see Table 3.6).

Table 4.5 Thematic analysis of answers to Q25. (Why do people have passwords?) (N = 37)

Theme Frequency (Percentage of Comments)	Sub-Theme Frequency (Percentage of Children Mentioning)	Examples Comments
What is the password protecting? (42, 32.8%)	Device, iPad, computer, mobile (23, 62.5%)	So my little brother do not use my device and programs (P39, G6)
	File, program (11, 29.7%)	So my little brother do not use my device and programs (P39, G6)
	Privacy and safety (5, 13.5%)	Has privacy in the device (P20, G6) it is safe and no one can penetrate (P30, G6)
	Account (2, 5.4%)	To secure our account (P1, G5)
	Something not specified (1, 2.7%)	So no one know (P24, G3)
Other's Action (41, 32%)	To gain access (31, 83.8%)	Because people do not know how to open it (P34, G1)
	To destroy (4, 10.8%)	Because none of the kids can play with my device or ruin it (P12, G1)
	To hack/steal/be curious (4, 10.8%)	So that nobody hacks them (P3, G5) Because some people are curious sometimes they access my stuff (P29, G4)
	To be able to search (2, 5.4%)	So no one can open my iPad or my computer to search (P14, G1)
Who? (37, 28.9%)	People in general (29, 78.4%)	To prevent others to log in (P5, G4)
	Other children (3, 8.1%)	So kids do not play with my device (P33, G1)
	The child (2, 5.4%)	Because I have privacy so no one access my things (P23, G2)
	My siblings (2, 5.4%)	My little brother Fares do not play with my iPad (P26, G2)
	Strangers, specifically people not known to the child (1, 2.7%)	Because people who we do not know do not use it (P25, G2)
Child's Action (8, 6.25%)	To prevent access (4, 10.8%)	To prevent others to log in (P5, G4)
	To be secure/to protect (2, 5.4%)	To secure our account (P1, G5)
	To create privacy (1, 2.7%)	Because I have privacy so no one access my things (P23, G2)
	To save things (1, 2.7%)	So they can save private things (P37, G3)

Table 4.6 Security words used in Q25 (Why do people have passwords?) (N = 10)

Security Words	Number of Children	Examples
Privacy/private (5, 50 %)	5 (Grade 2 - 6)	Has privacy in the device (P20, G6)
Protect (1, 10 %)	1 (Grade 4)	Protect the device (P17, G4)
Penetrate (1, 10 %)	1 (Grade 6)	It is safe and no one can penetrate (P30, G6)
Safe (1, 10 %)	1 (Grade 6)	It is safe and no one can penetrate (P30, G6)
Hack (1, 10 %)	1 (Grade 5)	So that nobody hacks them (P3, G5)
Secure (1, 10 %)	1 (Grade 5)	To secure our account (P1, G5)

4.3.2.2 Children's best practices while making passwords

In general, about three-quarters of the children said they have passwords (29/39, 74.4%). To use passwords appropriately one should have different passwords for different accounts. To explore this, the children were asked how many different passwords they have, the median number of passwords they report is two. The distribution of number of children having passwords shows an increasing number with age (see Table 3.7).

Table 4.7 Grade distribution of children who have passwords (N = 29)

Grade	1	2	3	4	5	6
Number of Children (%)	2/7 (28.6%)	4/6 (66.7%)	5/7 (71.4%)	6/7 (85.7%)	6/6 (100%)	6/6 (100%)

With regard to whether children change their own passwords at home or school, of the 29 children who have passwords, almost half (16[3]/29, 51.7%) did change their own passwords.

[3] One of the children who said he created his password had actually said in Q24 that he did not have any passwords. However, his answer is included here.

At school, of the four children who have passwords, half (2/4, 50%) changed their own passwords.

To investigate children's understanding of why strong passwords are used in the real world, a thematic analysis was conducted of the open-ended answers to Q26 (Why do you think that strong passwords are used in real life?). All the children answered this question, however one of the answers was irrelevant so it was excluded.

Table 3.8 summarizes the results of the thematic analysis, which used the same main themes of "What" is being protected, "Who" is it protected against and what actions by the child and others are relevant. In terms of who those others are, the "Who" main theme was mentioned by most participants, with the frequent response being "people in general" (71.1%); other less frequent responses included their siblings, other children, and hackers. The children also mentioned "What" is being protected by a strong password, most common categories were hardware (e.g., devices, iPads, computers, mentioned by (39.5%) and software (e.g., files, programs, also mentioned by 15.8%).

In terms of actions by others which a password might protect against, in this question the theme has been divided to "Other's Actions related to device" and "Other's action related to password". The most frequently mentioned action for Other's action related to device (47.4%) that the child thought that another person can do is to gain access to their device or information or to steal something (5.3%). While the most frequently mentioned action for Other's action related to password (18.4%) that the child thought that another person can guess their password or discover it (26.3%). Finally actions the child was taking by having a strong password was only mentioned by a small percentage of the children. Reasons for actions included wanting to have privacy (13.5%), to make themselves protect, prevent access, or save work (each 2.6%).

Also in this question only a minority of the children (6/38, 15.8 %) used security words (e.g., private, hacker); most of the children using such words are in the upper grades (4/6, 66.7 %) (see Table 3.9).

Table 4.8 Reasons given for Q26. (Why do you think that strong passwords are used in real life?) (N = 38)

Theme Frequency (Percentage of Comments)	Sub-theme Frequency (Percentage of Children Mentioning)	Examples Comments
Who? (35, 34%)	Someone/people (27, 71.1%)	Someone does not log in to your account (P1, G5)
	Sibling (4, 10.5%)	So my brother do not know it (P22, G2)
	Other children (2, 5.3%)	Because kids do not play with my stuff without my notice (P29, G4)
	Hackers (1, 2.6%)	So hackers cannot access mobiles (P20, G6)
	Strangers (1, 2.6%)	Because strangers do not remember it (P35, G5)
What is the password protecting? (24, 23.3%)	device/computer/mobile/iPad (15, 39.5%)	So hackers cannot access mobiles (P20, G6)
	Important data/information/my work (6, 15.8%)	To protect your devices and important data (P3, G5)
	Account (3, 7.9%)	Someone does not log in to your account (P1, G5)
Other's action related to device and/or its content (21, 20.4%)	To gain access (18, 47.4 %)	Because kids do not play with my stuff without my notice (P29, G4)
	Steals/ breach (2, 5.3%)	No one steals it (P4, G3)
	Search (spy) (1, 2.6%)	Because if someone has office key for others and try to search the computer they cannot (P14, G1)
Other's action related to password (20, 19.4%)	Unguessable (7, 18.4%)	Because people cannot guess it (P13, G4)
	Undiscoverable (10, 26.3%)	So my brother do not know it (P22, G2)
	Remember/ memories (2, 5.3%)	Because strangers do not remember it (P35, G5)
	Shoulder surfing (1, 2.6%)	Someone sees it from back do not remember it (P35, G5)
Child's action (3, 2.9%)	Prevent (1, 2.6%)	To prevent others to log in (P5, G4)
	Save (1, 2.6%)	Save my work (P10, G5)
	Protect (1, 2.6%)	To protect your devices and important data (P3, G5)

Table 4.9 Security words used in Q26 (Why do you think that strong passwords are used in real life?) (N = 6)

Security Words	Number of Children	Examples
Private (2, 33.3 %)	2 (Grade 2 and 3)	Because if it has your private things no one can access it (P23, G2)
Breach (1, 16.7 %)	1 (Grade 6)	So who want to breach my account will not do it easily (P30, G6)
Hacker (1, 16.7 %)	1 (Grade 6)	So hackers cannot access mobiles (P20, G6)
Prevent (1, 16.7 %)	1 (Grade 4)	To prevent others to log in (P5, G4)
Protect (1, 16.7 %)	1 (Grade 5)	To protect your devices and important data (P3, G5)

To further investigate children's understanding of passwords, they were asked to create a password that would be very easy to guess and password that would be hard to guess. The passwords created were analysed in four ways:

- Length: number of characters
- Composition in terms of letters, numbers and other characters.
- Use of meaningful elements (e.g., child's name) or obvious patterns (e.g., 10101).
- Language and alphabet used (Arabic/English/mix of the two languages, Arabic word in Latin alphabet).

Table 3.10 summarizes the length analysis for both easy and hard passwords. The number of characters and the range of lengths of hard passwords were higher than easy passwords, as expected. In both easy and hard passwords, more than 50% of passwords were composed of numbers only. However, 25% of hard passwords were composed of both numbers and letters, but 20.5% of easy passwords were composed of letters only. In relation to the use of meaningful patterns or elements, more than half of the easy passwords (66.7%) used a pattern, while only a quarter of hard passwords used a pattern (27.8%). On the other hand, about one fifth of both easy and hard passwords used a meaningful element (20.5% and 22.2% respectively). For language and alphabet aspects, English was used in over half both the easy and hard passwords (61.5% and 58.3% respectively), with only about a third of passwords being in Arabic. Only a small percentage of children used a mix of Arabic and English (2.6% for easy passwords and

8.3% for hard passwords). An interesting result was that one child used the Latin alphabet to write an Arabic word for his hard password (the child used “Aboooo199”, “Abo” in Arabic means “father of" in English).

Table 4.10 Analysis of the composition of easy and hard passwords created by the children in Study 1

Criteria of Comparing Passwords		Easy Passwords N = 39	Hard Passwords N =36*
Number of characters	Median	4.0	6.0
	Range	1 - 11	3 - 11
Composition	Numbers only	29 (74.4%)	21 (58.3%)
	Letters only	8 (20.5%)	3 (8.3%)
	Numbers and letters	1 (2.6%)	9 (25%)
	Letters, numbers, and special characters	1 (2.6%)	3 (8.3%)
Meaningful elements and patterns	Pattern (i.e., 10101)	26 (66.7%)	10 (27.8%)
	Element (i.e., name of child)	8 (20.5%)	8 (22.2%)
Language and alphabet	English	24 (61.5%)	21 (58.3%)
	Arabic	14 (35.9%)	12 (33.3%)
	Mix between Arabic and English	1 (2.6%)	3 (8.3%)
	Arabic word written in Latin alphabet	0 (0.0%)	1 (2.8%)

* Hard passwords from three children were not analysed as they did not provide an actual password only a description of the password.

In addition to the above analysis, password strength was measured using the zxcvbn.js password strength meter for the hard passwords only as it is worth to measure how strong suggested children's password. This is an open source tool widely used to measure password strength by giving a score from 1 (weak password) to 5 (very strong password)[4]. Table 3.11 shows the strength of participants password.

The meter revealed a high percentage of passwords with low strength (63.9% with a score of 2), as children used numbers only or short words (e.g., 8615, V1576, IENVEO). Only about a fifth of children (19.4%) created a password with high strength (score of 4) (e.g., Aboooo199, Od123os456). However, none of the passwords were rated as very strong (score of 5).

[4] https://www.bennish.net/password-strength-checker/
The meter does not retain password data to follow the ethical approval given for this study.

Table 4.11 Password strength of children's hard passwords created in Study 1

Strength Score	**1**	**2**	**3**	**4**	**5**
Number of Children (%)	4 (11.1%)	23 (63.9%)	2 (5.5%)	7 (19.4%)	0 (0.0%)

In addition, to understand the effect of different types of schools (state-funded school versus privately-funded school) on children's password creation ability, another analysis was conducted separately of easy and hard passwords created by children in each type of school (see Tables 3.12 and 3.13).

For easy passwords, the main differences between children from the two types of school were in composition and use of meaningful elements and patterns. In composition, children from state-funded schools were more likely to create passwords of letters only (26.3% vs 15%), whereas children from privately-funded schools also created more complex easy passwords (although numbers were small). Children from privately-funded schools were also more likely to use patterns in easy passwords than children from state-funded schools (75% vs 57.9%), whereas children from state-funded schools more likely to use elements than children in privately-funded schools (26.3% vs 15%).

Table 4.12 Analysis of easy passwords by children's school type

Criteria of Comparing Passwords		**State-Funded School N = 19**	**Privately-Funded School N = 20**
Number of characters	Median	4	4
	Range	1 - 11	1 - 11
Composition	Numbers only	14 (73.7%)	15 (75%)
	Letters only	5 (26.3%)	3 (15%)
	Numbers and letters	0 (0.0%)	1 (5%)
	letters, numbers, and special characters	0 (0.0%)	1 (5%)
Meaningful elements and patterns	Pattern (i.e., 10101)	11 (57.9%)	15 (75%)
	Element (i.e., name of child)	5 (26.3%)	3 (15%)
Language and alphabet	English	12 (63.2%)	12 (60%)
	Arabic	7 (36.8%)	7 (35%)
	Mix between Arabic and English	0 (0.0%)	1 (5%)

For hard passwords, children from both type of schools, largely created weak passwords (strength score of 2). However, more children from state-funded schools created stronger passwords than children from privately-funded schools, 33.3% of their passwords scored 4 compared to only 5.6% of passwords created by children from privately-funded schools. Other notable differences were that children from state-funded schools created hard passwords which were more likely to include numbers and letters (33.3% vs 16.7%) and more likely to include patterns. However, children from privately-funded schools also created more complex hard passwords.

Table 4.13 Analysis of hard passwords by children's school type*

Criteria of Comparing Passwords		**State-Funded School N = 18**	**Privately-Funded School N = 18**
Strength	1	1 (5.6%)	3 (16.7%)
	2	10 (55.6%)	13 (72.2%)
	3	1 (5.6%)	1 (5.6%)
	4	6 (33.3%)	1 (5.6%)
Number of characters	Median	6	5
	Range	4 - 11	3 - 10
Composition	Numbers only	10 (55.6%)	11 (61.1%)
	Letters only	2 (11.1%)	1 (5.6%)
	Numbers and letters	6 (33.3%)	3 (16.7%)
	letters, numbers, and special characters	0 (0.0%)	3 (16.7%)
Meaningful elements and patterns	Pattern (i.e., 10101)	6 (33.3%)	3 (16.7%)
	Element (i.e., name of child)	4 (22.2%)	5 (27.8%)
Language	English	11 (61.1%)	10 (55.6%)
	Arabic	6 (33.3%)	6 (33.3%)
	Mix between Arabic and English	1 (5.6%)	2 (11.1%)
	Arabic word written in Latin alphabet	1 (5.6%)	0 (0.0%)

* Hard passwords from three children (one in state-funded school, two in privately-funded school) were not analysed as they did not provide an actual password only a description of the password

To understand the effect of children's grade on ability to created passwords, another analysis done separately for easy and hard passwords (see Tables 3.14 and 3.15). As the number of children in each grade was small, grades were combined (i.e., Grades 1 and 2, 3 and 4, 5 and 6).

For easy passwords (Table 3.14), in terms of length, the median number of characters only increased from 4.0 to 5.0 across the grades, although the range increased from 7 characters to 11 characters. The other characteristics showed no clear trends, perhaps due to small numbers of children in each group.

Table 4.14 Analysis of easy passwords by children's grade

Criteria of Comparing Passwords		**Grades 1 & 2 N = 13**	**Grades 3 & 4 N = 14**	**Grades 5 & 6 N = 12**
Number of characters	Median	4.0	4.0	5.0
	Range	1 - 7	1 - 11	1 - 11
Composition	Numbers only	10 (76.9%)	12 (85.7%)	7 (58.3%)
	Letters only	2 (15.4%)	2 (14.3%)	4 (33.3%)
	Numbers and letters	1 (7.7%)	0 (0.0%)	0 (0.0%)
	letters, numbers, and special characters	0 (0.0%)	0 (0.0%)	1 (8.3%)
Meaningful elements and patterns	Pattern	8 (61.5%)	11 (78.6%)	7 (58.3%)
	Element	2 (15.4%)	1 (7.1%)	5 (41.7%)
Language and alphabet	English	7 (53.8%)	11 (78.6%)	6 (50%)
	Arabic	6 (46.2%)	3 (21.4%)	5 (41.7%)
	Mix between Arabic and English	0 (0.0%)	0 (0.0%)	1 (8.3%)

In hard passwords (Table 3.15), the percentage of weak passwords (scores 2 and 3) did decline from Grades 1 & 2 to the later grades, with a corresponding increase in stronger passwords (score of 4). There was no clear trend in number of characters, however compositions including numbers only decreased in higher grades (81.8% for Grades 1 & 2 vs 33.3% for Grades 5 & 6) with more complex compositions increasing, and the use of meaningful elements also increased (18.2% for Grades 1 & 2 and 33.3% for Grades 5 & 6).

Table 4.15 Analysis of hard passwords by children's grade. *

Criteria of Comparing Passwords		Grades 1 & 2 N = 11	Grades 3 & 4 N =13	Grades 5 & 6 N = 12
Strength	1	2 (18.2%)	1 (7.7%)	1 (8.3%)
	2	8 (72.7%)	7 (53.8%)	8 (66.7%)
	3	0 (0.0%)	2 (15.4%)	0 (0.0%)
	4	1 (9.1%)	3 (23.1%)	3 (25%)
Number of characters	Median	4.0	6.5	5.0
	Range	3 - 11	4 - 10	4 - 10
Composition	Numbers only	9 (81.8%)	8 (61.5%)	4 (33.3%)
	Letters only	2 (18.2%)	0 (0.0%)	1 (8.3%)
	Numbers and letters	0 (0.0%)	4 (30.8%)	5 (41.7%)
	letters, numbers, and special characters	0 (0.0%)	1 (7.7%)	2 (16.7%)
Meaningful elements and patterns	Pattern	3 (27.3%)	5 (38.5%)	1 (8.3%)
	Element	2 (18.2%)	3 (23.1%)	4 (33.3%)
Language and alphabet	English	5 (45.5%)	11 (84.6%)	5 (41.7%)
	Arabic	7 (63.6%)	2 (15.4%)	4 (33.3%)
	Mix between Arabic and English	0 (0.0%)	0 (0.0%)	3 (25%)
	Arabic word written in Latin alphabet	0 (0.0%)	1 (7.7%)	0 (0.0%)

* Hard passwords from three children (two in Grades 1 & 2, one in Grades 3 & 4) were not analysed as they did not provide an actual password only a description of the password

For each password type, children were asked what made the password they had created easy or difficult (Q29 and Q30). Table 3.16 summarises the results of a thematic analysis of children's answers for the easy passwords. The main themes were aspects of Composition of the password, accounting for half of the children's comments (50%); the Memorability/Guessability of the password, accounting for nearly a third of the children's comments (32%); and a Common Thing which the child knows, accounting for less than a quarter of the children's comments (18%).

In the Composition main theme, the most frequently mentioned sub-theme was having the same number or the same place to press when creating the password, mentioned by 8 children (20.5%). In the Memorability/Guessability theme, the sub-theme that other people can try guess was used moderately frequently (6, 15.4%), while most of the sub-themes referred to the child's ability to remember or recognise the password. In the Common thing that child knows theme, the most used sub-theme was the child's name (4,10.3%), followed by a family name (2, 5.1%), while name of a day in the week, name of things, mother's mobile password, and sequence of mobile number were all mentioned by one child (1, 2.6%).

Table 4.16 Thematic analysis of children's reasons for why the password they created is easy (N=39).

Theme Frequency (Percentage of Comments)	Sub-Theme Frequency (Percentage of Children Mentioning)	Example Passwords	Examples Comments
Composition **(25, 50%)**	Same number/same place to press (i.e., 111) (8, 20.5%)	111 000	Because it is the same numbers (P10, G5) I press the same place three times (P29, G4)
	Continuous numbers (7, 17.9%)	123456	Because numbers are continuous (P36, G3)
	Few characters (6, 15.4%)	121212	Few (P9, G6)
	First number (0) / (1) (4, 10.3%)	907 111	Because it is first number (P23, G2) One is the first number (P5, G4)
Memorability/ Guessability **(16, 32%)**	People can try (guess) (6, 15.4%)	1330549 [ChildName]	Means they try try try then they know it (P14, G1) Because all can guess my name (P7, G1)
	Remember (4, 10.3 %)	123456	Easy to remember (P2, G3)
	Easy in general / Simple (4, 10.3 %)	A551	Simple and easy (P21, G1)
	Known by others (2, 5.1 %)	[PartOfChildName PartOfFamilyName]	Because all knows that my password is 8 characters (P30, G6)
Common thing that the child knows **(9, 18%)**	Child name (4, 10.3 %)	[ChildName]	Because it is my name (P3, G5)
	Family name (2, 5.1 %)	[FamilyName123-]	Family name and start of numbers and the dash always used (P20, G6)
	Name of a day of the week (1, 2.6 %)	Monday	Because it is the second day of the week (P1, G5)
	Mother's password (1, 2.6 %)	66666	Because it is my mother password (P22, G2)
	Sequence of mobile number (1, 2.6 %)	50578	The same sequence of mobile number (P38, G2)

Table 3.17 examines from an adult perspective whether the children's answers explained logically why their password was easy, when compared with the created password. As the number of children in each grade was small, grades were combined (i.e., Grades 1 & 2, 3 & 4, 5 & 6).

Most children's (26, 66.7%) answers reflect the reason for chosen password (e.g., password: "Monday" and the reason "because it is the second day of the week[5]" (P1, G5)). While nearly a quarter (9, 23.7%) answers do not accurately reflect the reason for chosen password (e.g., password: "907" and the reason "because it is first number" (P23, G2) while "907" is the number of call centre for mobile company in Saudi Arabia). Overall, there was no significant trend in children's answers' reasonability depending on their grade (chi-square = 1.97, df= 2, p = 0.37)

Table 4.17 Comparison of children's easy passwords to their explanatory answers (Why it was an easy password?) by children's grade.

Child's Answer Matching his Password	Grade 1 & 2 N = 13	Grade 3 & 4 N = 14	Grade 5 & 6 N = 12	Total N=39
Reasonable answer	8 (61.5%)	8 (57.1%)	10 (83.3%)	26 (66.7%)
Not reasonable answer	5 (38.5 %)	6 (42.9%)	2 (16.7%)	13 (33.3%)

Table 3.18 summarises the results of a thematic analysis of children's answers for the hard passwords. The main themes were aspects of Composition of the password, accounting for almost half of the children's comments (55.6%); the Memorability/Guessability of the password, accounting for a third of the children's comments (33.3%), and a few comments related to Security issues and a Common Thing which the child knows, accounting for less than a quarter of the children's comments (6,7% and 4.4% respectively).

In the Composition main theme, the most frequently mentioned sub-theme was password having many characters, mentioned by 8 children (21.6%). In the Memorability/Guessability theme, the sub-theme that other people can try guess was used moderately frequently (7, 18.9%), while most of the sub-themes referred to the difficulty of numbers or to others to memorise the password. In the Security theme, the most frequently mentioned sub-theme was Shoulder surfing, mentioned by 2 children (5.4%). In the Common thing that child knows theme, name of family member and mobile number were each mentioned by one child (1, 2.7%)

[5] In KSA, the week starts on Sunday, so Monday is the second day of the week.

Table 4.18 Thematic analysis of children's reasons why the password is hard (N=37)

Theme Frequency (Percentage of Comments)	Sub-Theme Frequency (Percentage of Children Mentioning)	Example Passwords	Examples Comments
Composition (25, 55.6%)	Many characters (8, 21.6%)	123456	Because it is long (P29, G4)
	Not continuous numbers (8, 21.6%)	0852	Not sequence random (P38, G2)
	Combination (letters, numbers, or special characters) (7,18.9%)	V1576 e.1.2	Because it has letters and numbers (P9, G6) Because it use letters numbers and symbols (P2, G3)
	Same number/more than one place to press (2, 5.4%)	3670 05051163	Because I need to press more than one place (P28, G6) Because I repeat some of the numbers (P22, G2)
Memorability/ Guessability (15, 33.3%)	People can try (guess) (7,18.9%)	Pmznd	Means they cannot guess it (P14, G1)
	Difficult number (4, 10.8%)	8323	Difficult numbers (P24, G3)
	Known by child (2, 5.4%)	78myname34	Numbers means to me others could be not interested (P39, G6)
	Difficult to memorise (1, 2.7%)	Aas654321	They cannot memorise it (P11, G3)
	Easy to type (1, 2.7%)	351624	Easy to write it in the keyboard (P17, G4)
Security (3, 6.7%)	Shoulder surfing (2, 5.4%)	ارقام ملخبطه (random numbers)	Because if I enter my password, who's sitting beside me cannot know it (P34, G1)
	Encryption (1, 2.7%)	IENVEO	Because it is an encryption of something I know (P3, G5)
Common thing that the child knows (2, 4.4%)	Name of family member (1, 2.7%)	عزام	No one know my brother name (P7, G1)
	Mobile number (1, 2.7%)	(number of my aunt)	Because in our house only me who remember my aunt mobile number (P32, G4)

Table 3.19 examines from a logical adult perspective whether the children's answers explained logically why hard the password was hard, when compared with the created password. As the number of children in each grade was small, grades were combined (i.e., Grades 1 & 2, 3 & 4, 5 & 6).

Most children (22, 59.5%) answers reflect the reason for their chosen password (e.g., password: "e.1.2" and the reason "because it use letters numbers and symbols" (P1, G5)). While less than half of the children (15, 40.5%) answers do not accurately reflect the reason for chosen password (e.g., password: "78myname34" and the reason "numbers means to me others could be not interested" (P39, G6) while the reason could be combination characters). Overall, there was no significant trend in children's answers' reasonability depending on their grade (chi-square = 2.44, df = 2, p = 0.3)

Table 4.19 Comparison of children's hard passwords with their explanatory answers (Why it was hard password?) by children's grade.

child's Answer Matching his Password	**Grade 1 & 2 N = 13**	**Grade 3 & 4 N = 14**	**Grade 5 & 6 N = 10**	**Total N=37**
Reasonable answer	(7, 53.8%)	(7, 50%)	(8, 80%)	(22, 59.5%)
Not reasonable answer	(6, 46.2%)	(7, 50%)	(2, 20%)	(15, 40.5%)

4.3.2.3 Principles followed by children to create a password

Children were asked to select what makes a good password from a set of options (Q27), see Table 3.20. The most frequently chosen option was "Hard to guess" mentioned by 27 children (69.2%), closely followed by "easy to remember" (26, 66.7%). The least frequently chosen options were "has an easy clue" (mentioned by 6, 15.4%) and "name of famous person" (5, 12.8%).

The results for this question were also analysed in relation to school type and grade group. With regards to school type there was no significant difference in terms of frequency of choices (chi-square = 1.33, df = 7, p = 0.99) (see Table 3.21). Nor was there any significant difference due to grade (chi-square = 2.58, df = 7, p = 0.92) (see Table 3.22). As the number of children is small, they were grouped into levels of two grades.

Table 4.20 Children's selection of what makes a good password (N = 39)

Children's Selection	Frequency (%)
Hard to guess	27 (69.2 %)
Easy to remember	26 (66.7 %)
Easy to forget	16 (41.03 %)
Letters and numbers	14 (35.9 %)
Easy to copy	12 (30.8 %)
Simple	9 (23.1 %)
Has an easy clue	6 (15.4 %)
Name of famous person	5 (12.8 %)

Table 4.21 Children's selection of what makes a good password by school type

Children's Selection	State-Funded School N = 19	Privately-Funded School N = 20
Hard to guess	12 (63.2 %)	15 (75 %)
Easy to remember	14 (73.7 %)	12 (60 %)
Easy to forget	7 (36.8 %)	9 (45 %)
Letters and numbers	8 (42.1 %)	6 (30 %)
Easy to copy	6 (31.6 %)	6 (30 %)
Simple	5 (26.3 %)	4 (20 %)
Has an easy clue	3 (15.8 %)	3 (15 %)
Name of famous person	3 (15.8 %)	2 (10 %)

Table 4.22 Children's selection of what makes a good password by grade

Children's Selection	Grade 1 & 2 N = 13	Grade 3 & 4 N = 14	Grade 5 & 6 N = 12
Hard to guess	8 (61.5%)	9 (64.3%)	10 (83.3%)
Easy to remember	8 (61.5%)	11 (78.6%)	7 (58.3%)
Easy to forget	7 (53.8%)	4 (28.6%)	5 (41.7%)
Letters and numbers	3 (23.1%)	4 (28.6%)	7 (58.3%)
Easy to copy	5 (38.5%)	3 (21.4%)	4 (33.3%)
Simple	5 (38.5%)	3 (21.4%)	1 (8.3%)
Has an easy clue	2 (15.4%)	2 (14.3%)	2 (16.7%)
Name of famous person	3 (23.1%)	2 (14.3%)	0 (0.0%)

4.3.2.4 Adults role in creating and managing children's passwords

Parents were asked whether their child uses the Internet/ Web by themselves (Q13). Most parents (29, 76.3%) said that their child uses the Internet without parental help, while nearly a quarter (9, 23.7%) said that their child gets help from a parent to use the Internet, and one parent did not answer this question. There was no significant trend in children's independent use of the internet depending on their grade (chi-square = 0.98, df = 2, p = 0.61) (see Table 3.23).

Table 4.23 Children's use of the Internet with or without parental help by grade

Use of Internet	Grade 1 & 2 N=12	Grade 3 & 4 N=14	Grade 5 & 6 N=12	Total N=38
Without parent help	8 (66.7%)	11 (78.6%)	10 (83.3%)	29 (76.3%)
With parent help	4 (33.3%)	3 (21.4%)	2 (16.7%)	9 (23.7%)

Parents were asked whether they use a password to log in to systems which their child then uses (Q20). Most parents (31/39, 91.2%) indicated that they did login for their child. On the other hand, a small number of parents (3/39, 10.3%) indicated that they do not use passwords for their child. There was no significant difference depending on school type schools (chi-square = 2.6, df = 1, p= 0.11) (see Table 3.24). In addition, there was no significant trend with grade (Table 3.25, chi-square = 0.02, df = 2, p = 0.99).

Table 4.24 Parental login for their child by children's school type*

Child's Password	State-Funded School N=15	Privately-Funded School N=19
Used by parent	15 (100%)	16 (84.2%)
Not used by parent	0 (0.0%)	3 (15.8%)

* Five of the children whose parent login to a system using child's password, actually their children said in Q24 that they did not have any passwords. However, their answer is included here.

Table 4.25 Parental login for their child by children's grade

Child's Password	Grade 1 & 2 N=10	Grade 3 & 4 N=12	Grade 5 & 6 N=12
Used by parent	9 (90%)	11 (91.7%)	11 (91.7%)
Not used by parent	1 (10%)	1 (8.3%)	1 (8.3%)

Parents were asked whether they create passwords for their child (Q21). About half the parents (17/39, 58.6%) answer that their child creates their password on their own, without the parent's involvement. However, the other half (16/39, 41%) indicated that one of the parents creates passwords for their child. There was no significant difference due to school type (chi-square = 0.02, df= 1, p= 0.88, see Table 3.26). Nor was there any significant trend with grade (chi-square = 0.41, df = 2, p = 0.81, see Table 3.27).

Table 4.26 Parental creation of passwords for their child by children's school type*

Child's Password	State-Funded School N=14	Privately-Funded School N=19
Created by child	7 (50%)	10 (52.6%)
Created by parent	7 (50%)	9 (47.3%)

* Four of the children whose parent said they create their children's password, actually their children said in Q24 that they did not have any passwords. However, their answer is included here.

Table 4.27 Parental creation of passwords for their child by children's grade

Child's Password	Grade 1 & 2 N=9	Grade 3 & 4 N=12	Grade 5 & 6 N=12
Created by child	4 (44.4%)	6 (50%)	7 (58.3%)
Created by parent	5 (55.6%)	6 (50%)	5 (41.7%)

4.3.3 RQ3: Do Saudi children have problems in relation to password creation in Latin alphabet and in English?

Parents were asked how many English words their child knows (Q22). This is relevant to password behaviour as children may be required to create passwords using the Latin alphabet. Thus, knowing children's level of English might assist to understand if it has an effect on passwords created at when children were asked to create an easy and hard password (Q28). All 39 parents answered this question using description words or range of numbers (see Table 3.28). Answers were grouped into categories according to the most used word or number. More than third of parents (35.9 %) indicated that their child knows less than 40 words and on similar percentage (35.9%) other parents indicated their child knows a range of 40-100 words. A small number of parents (12.8%) also indicated that their child knows an "excellent" vocabulary. Less than 10% of parents (7.7% in each case) said the number was in the range of 100-200 words or "Good". As this question was an open-ended question, the responses varied between description words or numbers. In hindsight, it would have been more appropriate if it

was in a multiple choice form. Thus, further statistical analysis could not be conducted based on school type or grade.

Table 4.28 Parent's answers on number of English words known by children in the study (N=39)

Number of Words	Number of Children (%)
Less than 40	14 (35.9%)
40-100	14 (35.9%)
100-200	3 (7.7%)
Good	3 (7.7%)
Excellent	5 (12.8%)

4.3.4 RQ4: At what age do Saudi parents think it is important for their children to understand how to make passwords for online systems?

Finally, parents were asked whether they think it is important for their child to understand how to make passwords for online systems (Q23). Over half of the parents (23, 59%) did think it important, while the rest did not. However, this answer varied significantly depending on the child's grade (see Table 3.29, chi-square = 10.8, df = 2, p= 0.005). Parents of older children were more likely to think it important that their child understand how to make passwords, with 83.3% of parents of children in Grades 5 or 6 agreeing, compared to only 23.1% of parents of children in Grades 1 or 2.

Table 4.29 Parents' opinion of the importance of their child understanding how to make a password for online system by children's grade

Parents' Opinion	Grade 1 & 2 N=13	Grade 3 & 4 N=14	Grade 5 & 6 N=12	Total N=39
Important for the child	3 (23.1%)	10 (71.4%)	10 (83.3%)	23 (59%)
Not important for the child	10 (76.9%)	4 (28.6%)	2 (16.7%)	16 (41%)

4.4 Discussion

Children from early age urgently need to understand password best practices that will help them to be prepared properly when they grow up. In the absence of educational lessons regarding security practices in the Saudi Arabian curriculum for children aged 6-12 years, the present study aimed to investigate four main research questions. The first (RQ1) concerned Saudi children usage of digital devices, the second (RQ2) concerned Saudi children's understanding of the use of passwords and their knowledge of security best practices in relation to passwords, the third (RQ3) related to language barriers to non-English speakers (specifically Arabic speakers) and its effect on password creation, and the fourth (RQ4) focused on Saudi parents' opinion of the importance of knowing about how to make a password to their children. The results on these four questions are addressed in the following sub sections.

4.4.1 Saudi children's use of password and digital devices at home and at school

All the children use digital devices at home and about half (56.4%) at school. This is not surprising, given these children were born in the 2010s, when digital devices had become very widely used in KSA. The results indicated that tablet computers are the most used at home (71.8%) while desktop computers are most used at school (95.5%). This high use of handheld devices in turn facilitates the more common online activities (Anderson and Jiang, 2018), indeed, all children in this study use digital devices at home for gaming and nearly all (87.2%) for entertainment. As a result, children experience a great need for authentication: most of children (88 %) have passwords for digital devices at home while only (18.2%) at school.

4.4.2 Saudi children's understanding of the reason for passwords and how to create them

In this study the children demonstrated a general understanding of the purpose for using passwords. Mostly they want to avoid other's actions (33.1%), with preventing access having the highest percentage among children's answers (86.5%). Overall children's greatest understanding is to prevent access to their devices or files, this was confirmed also by Read and Cassidy (2012), however, none of the answers in this study were "to allow access to legitimate person". In addition, most older children (63.2%) indicated that strong password help to protect their devices or its content from other people, while most younger children

(60%) indicate it will protect their password from other people. Previous research has shown that children in the 6 to 12 age range seem to be confused by the concepts related to passwords: privacy and safety, and protection (Choong et al., 2019a; Theofanos et al., 2021), and in this study only few children (21.6%) use words like privacy or secure. It is interesting to find that most (81.8%) of the security words were used by older children (Grade 4 - 6) in their answers (e.g., prevent, protect, hacker, etc) which confirmed the result from Coggins (2013). While younger children might mean the same thing in what they say, but not the actual terms. Hence, this reflects the different cognitive abilities between younger and older children.

Children in this study created hard and easy passwords, these were examined in term of number of characters, composition, use of meaningful elements, and language and alphabet used. In addition, both easy and hard password were compared according to age group and type of schools, to study the effect of cognitive ability and the English level of children. There were differences revealed in the results related to age group, however, in regard to English level (as measured to school type) no significant differences were revealed. When comparing both passwords, easy password has less characters, as expected (median for easy password 4 characters, while for hard password 6 character) however, in both cases these would be considered short passwords (Ratakonda et al., 2019). This can perhaps be explained by the children's answers on the type of password structure that they use in their devices: most were passcode or password containing numbers only and the length between 4 to 6 characters. As all the children play games, most probably on a game console or tablet that requires passcodes of 4 to 6 numbers only. A higher percentage of children used numbers or letters only in their easy password than in their hard password (74.4% and 20.5% respectively). On the other hand, a higher percentage of children used complex passwords (i.e., letters and number, or letters, numbers, and special characters) in their hard password (33.3%) than in their easy password (5.2%). In this instance, children showed a good understanding of some of the security best practices. A pattern used more by children in their easy password (66.7%), while self-related information was used almost equally in both easy and hard passwords (20.5% vs 22.2%). This could be related to their memorability, a factor confirmed by other researchers (Lamichhane and Read, 2017; Maqsood et al., 2018; Read and Cassidy, 2012). Furthermore, in this study the results showed that children struggled to create a strong password with only 19.4% creating a genuinely strong password. Most of children who did so were in the older age group (9-12 years) and from stated-funded school. It was surprising to find that more than half of the strong

passwords contains self-related information about the child but the password strength meter could not identify is because it contains (Arabic name of child written in Latin alphabet, date of birth using Gregorian calendar, or Saudi mobile number).The reason could be that most of password strength meters are based on English dictionaries (Darbutaite et al., 2023; Hong et al., 2021) while to my knowledge no password strength meters are based on Arabic dictionaries. In term of the language used to create a password, children mostly used English language in both easy and hard password with no significant difference with regard to type of school. In addition, it is interesting to find that in both type of passwords, most younger children (6-8 years) used Arabic language compared with one from the English language. Nevertheless, some children (8.3%) in making their hard password used a mix of Arabic and English language compared to very few (2.6%) in making their easy password. More specifically, most children who used a mix between Arabic and English language in their hard password are in the older age group (10-12 years) and from private-funded school. It was particularly surprising to find a child from state-funded school making a hard password using an Arabic word written in Latin alphabet. The children already had a sense of the general characteristics of password as evidenced by their answers of why they consider their password to be easy or hard. The children recognised that the strength of a password depends on its composition, this was the most theme used in comments for both easy as hard passwords (50% and 55.6% respectively), the memorability theme was the second highest occurring theme (32% for easy password and 33.3% for hard password). Furthermore, the children considered using common words (e.g., child name) could make their password easy or hard, but due to their age and lack of education they did not take into account the security issue of having these types of words in their password. The security theme was used only in hard passwords with a low percentage of comments (6.7%), indicating that those children have some awareness of what constitutes a strong password which confirms Coggins (2013) result. In fact, some of the children's answers did not match the password they created (either the easy or hard password), this percentage was low amongst older children (10-12 years), but higher amongst younger children (6-9 years). This could be because with their level of cognitive capability at these ages they cannot always express their answers logically or it is not clear for them what a password should consist of.

Lamond et al. (2022) refer to "objective knowledge" as the actual knowledge while "subjective knowledge" as perceived knowledge. The results show inconsistencies between children's

subjective and objective knowledge, which is the same for adults, but it is not clear from the literature review (Chapter 2, section 2.3 and 2.4) to which extent the inconsistencies between subjective and objective knowledge are the same for adults when compared with children. Most children actually created weak password, while theoretically indicating that they know what a strong password is. For example, when answering Q27. (What makes a good password?) 69.2% of the children indicated that a password should be hard to guess, 35.9% indicated they should use mix between letters and numbers, and 87.2% did not choose the option "Name of famous person" as a choice. This result was also confirmed by other researchers (Choong et al.,2019a, b; Ratakonda et al., 2019; Theofanos et al., 2021), who found that these differences decreased with age.

Almost half of children rely on their parent to create their password, 23.7% of children get help from their parent to access the Internet, and 91.2% of parents use children's password to access their child's account or device. With this high percentage in relying on parents and without having an education curriculum at schools regarding security practices, adults (i.e., family member, teacher, or friends) will be the only resources for children to learn about good security practices. Unfortunately, in this study I did not collect information from teachers or demographic information about parents to further investigate this issue. In some cases, children can be unreliable informants and if I had the chance, I would have added more follow up questions to this study.

4.4.3 Saudi children and the use of Latin alphabet in password creation

The number of words that children know in their native language in Grade 1 and 2 approximately 13,000 words, while in Grade 3, 4, and 5 it is between 20,000 and 40,000 words (Merritt, 2016). Spelling mistakes and memorability issues are among the top challenges for children in creating and using passwords (Cole et al., 2017; Lamichhane & Read, 2017; Read & Cassidy, 2012; Stewart et al., 2020). In this study all the children speak and write Arabic as their first language and most of the children (79.5%) know 200 words or less of English (although my measurement of this by asking parents was very subjective). Unfortunately, some websites only accept the use of Latin alphabet in creating passwords, it is clear that language will affect children's ability to create their own passwords. On the other hand, those websites which accept the use of the Arabic alphabet have two major issues: first, if a child uses the Arabic alphabet then the numbers should be in Arabic numerals as used with the Latin alphabet

(e.g., 4) and not Eastern Arabic numerals that is used by Arabic native speakers (e.g., ٤), so the child will need to move between two language on the keyboard. Second, the use of the Arabic alphabet may not be secure because password strength meters do not recognise the Arabic alphabet and consider a password to be strong even if it has only letters (e.g., Monday in the Arabic alphabet).

4.4.4 Saudi parent's opinion of the importance of their child understanding how to make passwords

It is a good indication to see that parents are thinking positively about their children's education in relation to security practices. The results of this study revealed a high percentage of parents supporting the importance of having their child understand password creation by following security best practices. Parents of older children (10-12 years) were more likely to think it important that their child understand how to make passwords. Hence, parent, teachers, and children themselves share the responsibility to teach children to understand cybersecurity (Lorenz et al., 2018). By providing them with needed support and guidance from cybersecurity specialist and educational curriculum providers.

To sum up, the main findings of this study are that children have a good understanding of security best practices, but they do not know how to apply them. This is clear from the passwords created in this study and the children's explanations in the open-ended questions. Other findings which were surprising in this study were: firstly, children's general understanding of passwords is "to prevent access of others" while no child answered that they were "to allow access to legitimate user". Secondly, some children created their password using Arabic word but written in the Latin alphabet; this would cause a password strength meter to consider it a strong password, but it may be a common word in Arabic. This is because existing strength meters are based on English dictionaries and do not use Arabic dictionaries. Thirdly, when comparing children based on their school type, it was expected that children who attended privately-funded schools would have stronger passwords compared with children attending stated-funded schools, but the results were the opposite.

The main limitations of the study were, firstly, the open-ended questions in this study had the same language and format for all age groups. However, in some cases, the younger children found it difficult to answer the open-ended questions. It would have been better to make the

format and language of questions more appropriate for each age group, and have different questions for younger and older children. Secondly, although at the beginning of this study it was planned to conduct this study with children from Saudi Arabia and UK to compare the results, however, due to the mode of my study (distance learning) this goal could not achieved. Thirdly, demographic information about the parents interviewed was not collected.

4.5 Conclusions

To conclude, children in Saudi Arabia interact with different digital devices and most have a password either for their devices, online accounts, or both. To some extent they have a good understanding of security practices theoretically, but unfortunately, practically they do not apply this understanding correctly. Password are difficult for children and need specific cognitive capability that they have not yet developed. Forcing children to create and use strong passwords is difficult cognitively for children in the age range of 6 to 12 years. Even if we ask children to make an easy password, this password could be remembered but hard for them to spell. Parents are doing their best to educate their children and support them about security practices, more than half of parents in this study (59%) think it is important to educate children about security best practices and almost all (80%) know their child's password and login to keep track of their activities. However, I am not sure what educational background related to cybersecurity do parents have. In addition to password challenges for children in general, Arabic children struggle more due to lack of academic curriculum at schools and their literacy in the English language. Therefore, knowing that children have difficulties using the Latin alphabet from this study and other studies discussed in the literature review, it was important to investigate age-appropriate authentication systems. This included avoiding using the Latin alphabet due to children's levels of literacy in English, and be compatible with their levels of literacy in their own language, their cognitive ability and memory development. Thus, graphical authentication systems suitable for children needs are presented in Chapters 4 and 5.

Chapter 4

Study 2: DoodlePass: An Authentication System Suitable for Children

5.1 Introduction

Younger children increasingly use the Internet and digital devices, especially since the COVID-19 pandemic and the transformation from physically attending classes to online classes. This therefore requires the use of authentication systems to access devices and accounts. It has been shown in the literature review (Chapter 2) and Study 1 (Chapter 3) that the use of passwords is challenging, particularly for non-English native speakers and in general for all children aged 6 to 12 years as they are still developing their cognitive, memory, and linguistic capabilities. In fact, the secure use of text passwords requires a full understanding of text password best practices starting from how to create a strong password, through skills to how to remember it, ending with how to avoid sharing it and maintain confidentiality. From Chapter 3, it was clear that children have a general understanding of security best practices, but they could not apply them correctly when creating their text passwords, this may be because text passwords are not suitable for the children's cognitive ability (Assal et al., 2018). Another challenge for children discussed in the literature review (Chapter 2, section 2.6) is recalling text password and their ability to remember it for long term taking into account their level of memory development. Thus, graphical authentication systems are worth exploring as one of the possible alternative systems to text password authentication systems for children. Using such systems will also help to introduce the concept of authentication systems to children using procedures that are within their skills. Younger children are at the egocentric stage of cognitive development (see Chapter 2, section 2.2) and using children's own drawings is within their realm of self-related information that is suitable for this cognitive stage of their development (Renaud, 2009; Stewart 2020). In addition, it will help to avoid the linguistic issues related to creating text passwords and remembering how to spell them when entering them. Most

importantly, graphical authentication systems rely on recognition rather than recall which is more appropriate for children's level of memory development.

In this chapter, a graphical authentication system called DoodlePass was developed and evaluated with 37 children aged 6 to 12 year from a private international school and a state-funded school at Saudi Arabia. This is similar to the research reported by Renaud (2009a) as she used doodles with children aged 11-12 years, but the details of the system, age group of the children and the method of evaluation of the system are different from her previous research. The DoodlePass authentication system is a web-based system which uses children's own drawing (simple doodles). In the most complex version of the system, children need to select three of their own doodles in the same order to be authenticated. The system has been evaluated for short-, medium-, and long-term effectiveness, efficiency and satisfaction and the results were promising. Most children remembered their DoodlePass in the correct order and the majority of children preferred to use DoodlePass more than a text password.

This study addressed the following research question:

RQ5: Is the DoodlePass authentication system usable by children aged 6 to 12 years?

5.2 Method

5.2.1 Design

The study used a mixed design, with one between-participants independent variable and two within-participants independent variables. The between-participants variable was the school grade of the children, which ranged from Grade 1 (6 – 7 years old) to Grade 6 (11 - 12 years old) (see Table 4.1). The first within-participants variable was complexity of the DoodlePass authentication system, which involved one, two or three doodles (i.e., simple drawings). The doodles were drawn by the children at the beginning of the study. The second within-participants variable was the login occasion to recognise and selecting DoodlePass, with four levels: recognition after creating the DoodlePass (Immediate Recognition); recognition after 10 minutes with distraction (playing a video game) (Short Term Recognition); recognition after approximately one week (Medium Term Recognition); and recognition after nine months (Long Term Recognition). Originally the plan had been to have the final session three months

after the first group of sessions, but the COVID-19 pandemic started in the middle of the three month period, so the final session had to be delayed. In addition, due to the ongoing pandemic, the pre-session and the first four experimental sessions were conducted face-to-face with the children, but the final session was conducted via Zoom.

The DoodlePass authentication system tested the children's ability to correctly recognise their own doodle displayed in a series of 3 x 3 grids with a range of distractor doodles (see Figure 4.3), thus creating a child-appropriate authentication system. To ensure usability, a 3 x 3 grid size was chosen for DoodlePass. This is to make it easy for the children to see all the doodles together. Mendori et al. (2002 & 2005) suggested using a smaller number of images in a grid, between 8 and16 images, to make the interface suitable for children to choose from in terms of efficiency and effectiveness. However, there was no further guidance found in the literature regarding grid size.

The dependent variables were the accuracy of recognition of the doodles in the authentication system and the time taken to recognise the doodles. For the two and three grid doodles, accuracy included both correct recognition of the doodles and remembering the correct order of doodles in the grids.

The study involved a Pre-Session and five experimental sessions, each approximately one week apart (see Figure 4.1), apart from the final session which was approximately nine months after the previous session.

Each session introduced a more complex authentication system (see Figure 4.2). The child's doodles act as the authentication key, that is the information they need to recognise and select to authenticate themselves and log in. The authentication key or authentication doodle was increased from one to two to three doodles as the study progress. This allowed the investigation of children's recognition of increasingly more complex authentication keys, their recognition of the keys over different periods of a time (a week and for the final three doodle authentication key (DoodlePass:3), over a period of approximately nine months). In addition, this was parallel to text passwords in terms of having more than one component to construct the authentication key.

At the Pre-Session, the children each created three different doodles using an iPad, so there would be sufficient doodles for all three authentication keys of the DoodlePass authentication system.

Each experimental session consisted of a number of parts (see Figure 4.1), these parts happened in different orders, depending on the session:

- Children choosing one of their doodles for the appropriate authentication key of DoodlePass.
- Logging into a video game system using the DoodlePass. This tested the children's ability to recognise and select their DoodlePass.
- Playing an online video game for 10 minutes. This acted as both a reward, distractor, and justification of the study for the children.
- Logging in again after playing the video game. This was used either to increase complexity of the authentication key by adding more doodles to the DoodlePass or to test the children's ability to recognise and select their DoodlePass.
- Answering questions about their use of computing devices, and their knowledge and use of text passwords and authentication systems. It was decided to spread these questions out over the different sessions, to avoid overwhelming the children with too many questions at one time (see Table 4.3).

As the targeted sample of participants in this study are 6-12 year old children, according to Piaget's development theory (Chapter 2, section 2.2) most of participants would be at the concrete operational stage (Grades 2 – 5, ages 8-10 years) while only one grade of children would perhaps be at the preoperational stage (Grade 1, age 6 years) and one grade of children at the formal operational stage (Grade 6, age 12 years). Thus, the design issues considered in this authentication system were based on children's general cognitive abilities at the concrete operational stage as follows:

1. Participants were given full and clear instructions on what they need to draw at the first stage and the importance of their DoodlePass to access the game.
2. The interface of the system was designed to be familiar to the children, such as 3 x 3 grid is the same as the authentication interface of tablets (most the used digital device

as found in Chapter 3, section 3.3.1.1) and all doodles were presented in the same grid rather than using tabs.

3. The interface should have only one button on each page, be simple, with light background colour to help reduce cognitive load for children and avoid confusion.
4. Children may get frustrated if they choose an incorrect doodle, thus in this system they had the chance to enter their authentication key for four attempts with a hint from the researcher only after three unsuccessful attempts.
5. The authentication key was based on the child's own drawings (doodles) rather than text to avoid spelling mistakes and to ensure long term memorability.
6. Young children do not know how to keep a secret, the use of doodles meant it would be difficult for children to describe their authentication key to others.
7. To ensure children's engagement and continued participation in all sessions of the study, their names appeared in the interface as soon as the researcher entered the child's code (username), in addition I emphasised the importance of securing their game with an authentication key.

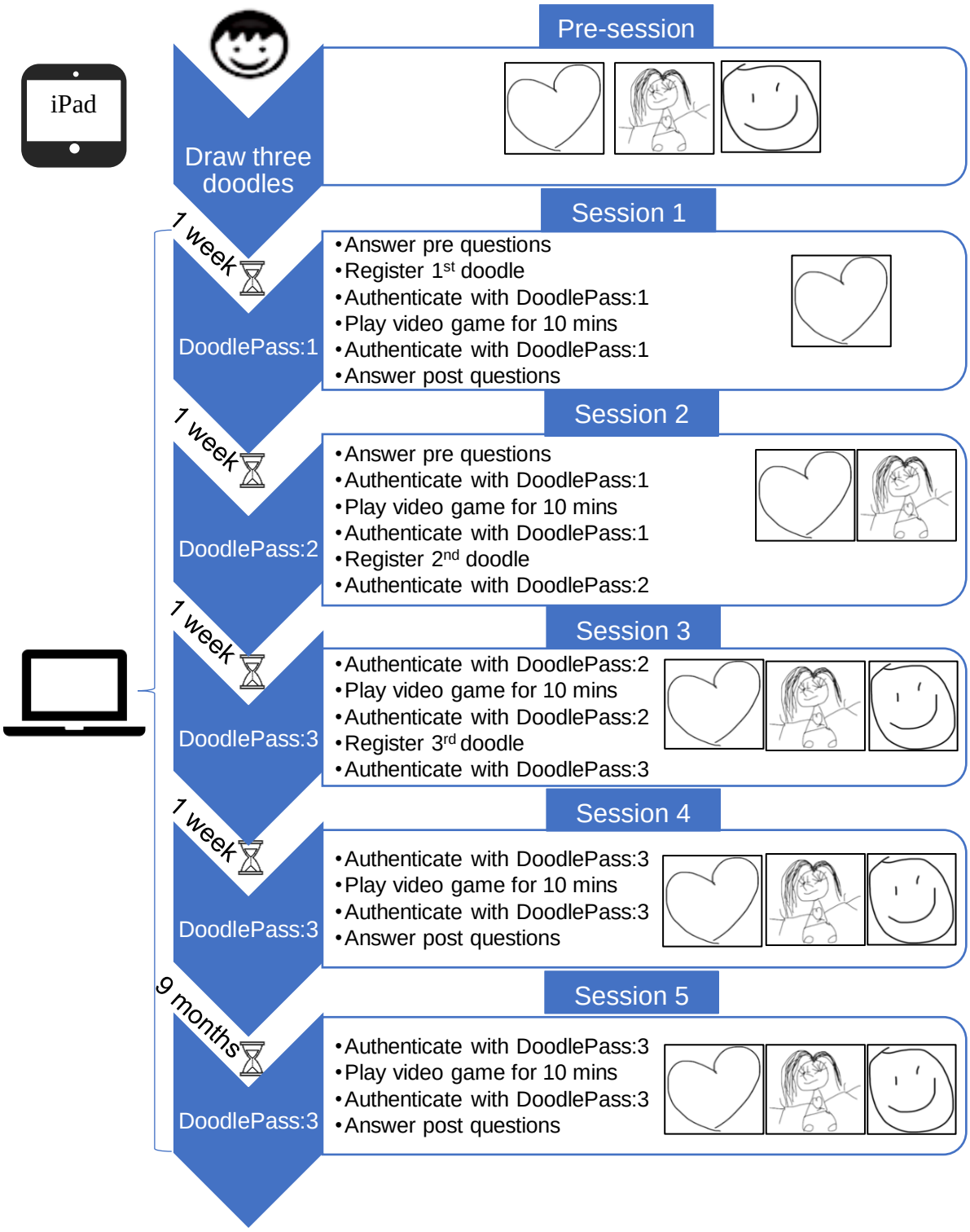


Figure 5.1 Overview of the design of DoodlePass authentication system

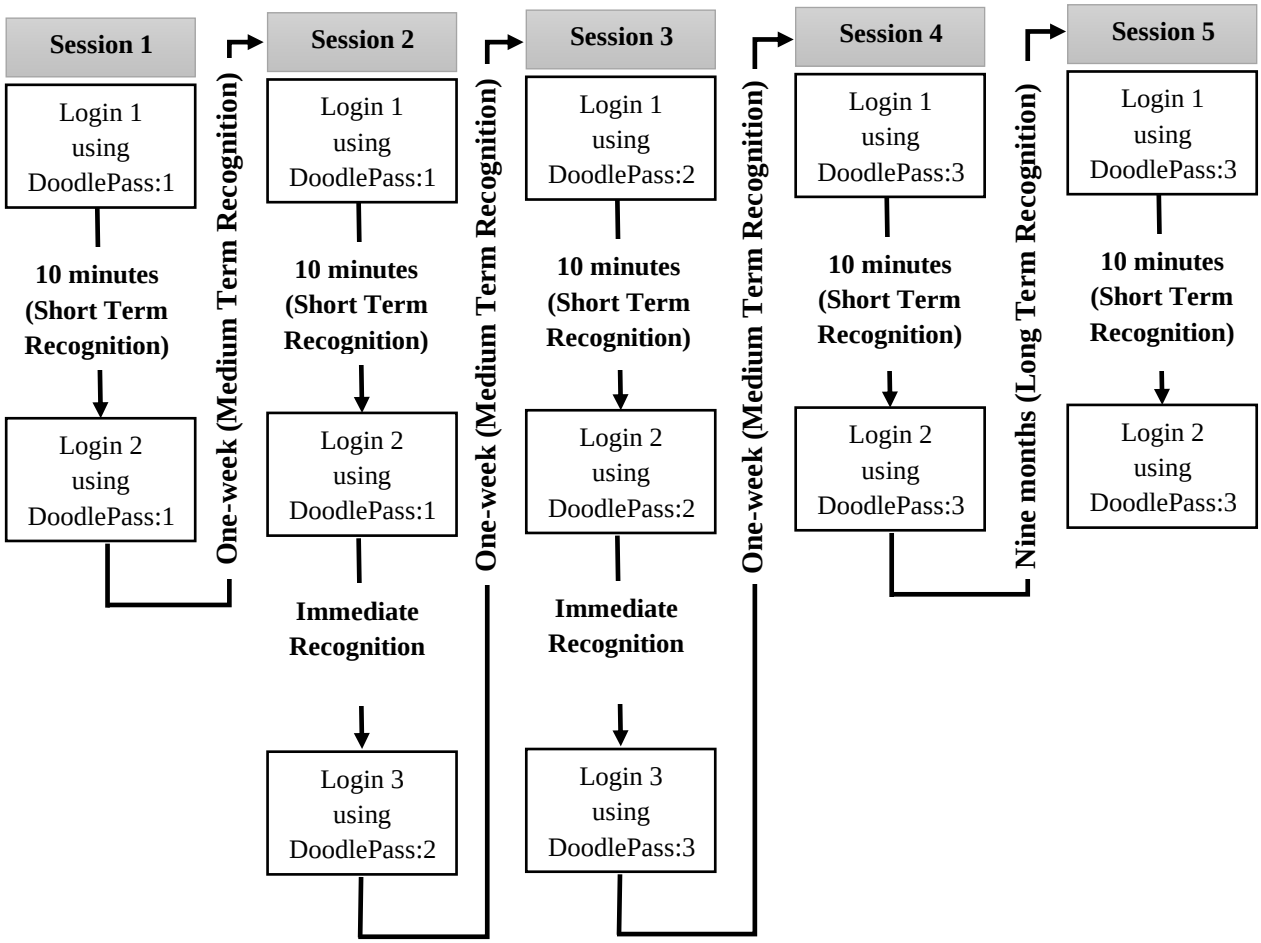


Figure 5.2 Login distribution and authentication key in each session at DoodlePass authentication system

5.2.2 Participants

37 children took part in the Pre-Sessions and experimental Sessions 1 and 2, all were recruited from a private international school and a state-funded school in Saudi Arabia. The children comprised 19 boys and 18 girls and were aged from 6 to 12 years (see Table 4.1). All the girls, and the boys in Grades 1 to 3, were at the private international school; the boys in Grades 4 to 6 were at the state-funded school (see Appendix A.4 for more details regarding the differences between private international school and state-funded schools in Saudi Arabia in term of English and computer curricula). The choice of Saudi children was because I was undertaking by PhD as a distance learning student, so I conducted my empirical work in my own country Saudi Arabia while also working at the University. So Saudi children were the only children available to me to participate in this study.

All 37 children had some experience with passwords and authentication systems, either for accessing digital devices or online accounts. One child initially said he had no experience with

passwords, but in subsequent questions said he did, so it is assumed that he answered incorrectly to the first question (perhaps he was nervous because this was the first question asked). 34 children (40.5%) had used password for digital devices only, a further 19 (51.4%) used them for digital devices and online accounts and two children (5.4%) used them for online accounts only. The children used a range of digital devices, the most popular being smartphones, used by 26 (70.3%) of the children, followed by tablet computers (used by 18, 48.6%), game consoles (13, 35.1%) and desktop/laptop computers (12, 32.4%).

However, in Session 3 (at the beginning of the COVID-19 pandemic) 34 children attend, and week later for Session 4 only 27 children attend. In the fifth session (nine months after the beginning of the study) only 22 of the children returned to complete the study (see Table 4.2). Due to the time lapse, the children had moved up to the next grade in school. Table 4.2 shows the children in the grades they were in for Sessions 1 to 4, but with their new grade also indicated.

Table 5.1 Distribution of participants in Pre-Session and Sessions 1 to 4 for the DoodlePass authentication system

Grade	Age (Years)	Gender Distribution	Number of Participants
1	6-7	3 boys, 3 girls	6
2	7-8	3 boys, 3 girls	6
3	8-9	4 boys, 3 girls	7
4	9-10	3 boys, 2 girls	5
5	10-11	3 boys, 4 girls	7
6	11-12	3 boys, 3 girls	6
Total		19 boys, 18 girls	37

Table 5.2 Distribution of participants in Session 5 for the DoodlePass authentication system

Grade	Gender Distribution *	Number of Participants
1 -> 2	3 boys, 2 girls	5
2 -> 3	3 boys, 1 girl	4
3 -> 4	4 boys, 3 girls	7
4 -> 5	-	0
5 -> 6	4 girls	4
6-> 7	2 girls	2
Total	10 boys, 12 girls	22

* As the final session was nine months after Session 4, the children had moved to the next grade

The children were offered a gift voucher worth 50 Riyal (approximately USD 13) to spend at a local bookstore for participating in the study.

5.2.3 Materials and equipment

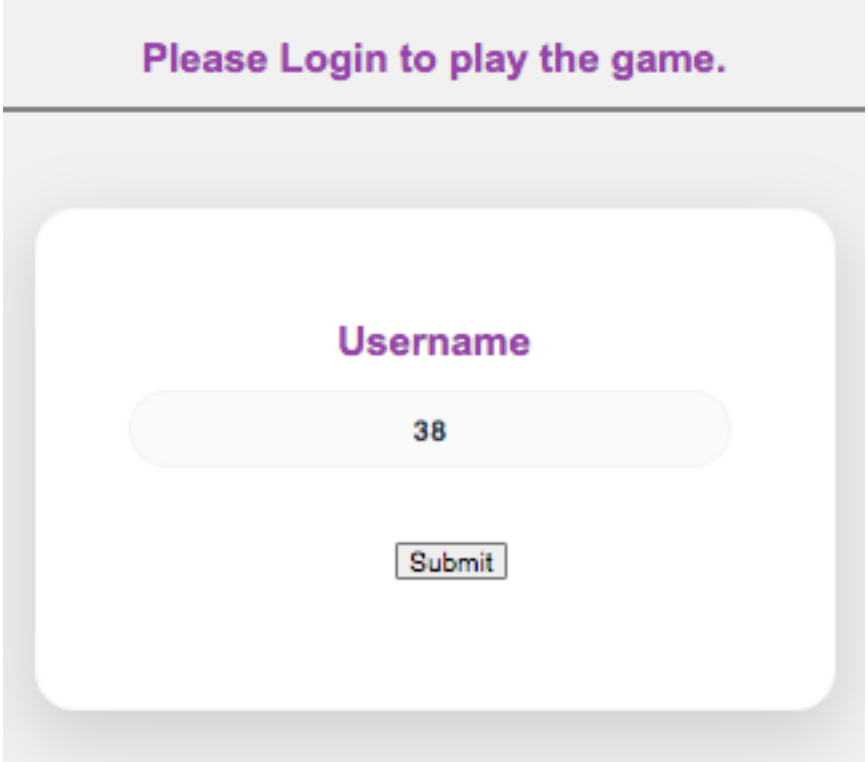
A website was developed to present the DoodlePass authentication system, to give children access to a range of age-appropriate video games and to collect data about the accuracy and timing of their responses to the DoodlePass authentication system.

The website has two versions (Arabic and English). The English version was used with the children in the private international school, as their level of English is good. The Arabic version was used with the children in the state-funded school, as their level of English is not as good. Each child used the same version throughout the study. Figures 4.3 and 4.4 illustrate pages from the website in both English and Arabic.

The website was developed using PHP, JavaScript and XML with a MySQL database. The website starts with a page in which the researcher enters the child's code, so session information is correctly stored (see Figure 4.3). Then the child is transferred either to a login page or an authentication key registration page. These both have "Welcome" and the child's name at the top of the page, to give the child confidence that the site has recognised them.

On the authentication key registration page, the child constructs their DoodlePass, by choosing one of their doodles. This is required in the first three sessions (see Figure 4.5).

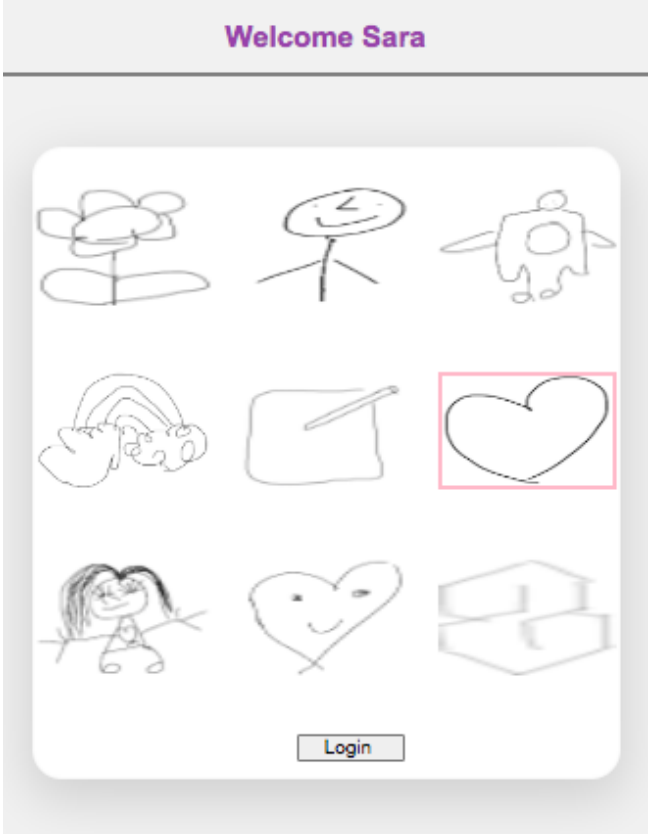
The login page is to allow the child to use the DoodlePass authentication system. It consists of one, two or three pages for authentication, depending on which authentication key is being used at the time. Each page contains a 3 x 3 grid that includes the child's authentication key, one of the other two remaining doodles created by the child (to ensure that the child knows the correct order), a doodle in the same category created by another child participating in the study (to ensure that the child could recognise their own hand drawing and not the name of the doodle), and other randomly selected doodles from other children participating in the study. When a child selects a doodle as their authentication key, it is highlighted by a box so the child can see which doodle they have selected and change their mind about their selection if they wish, before attempting to log in (see Figure 4.4). The login pages are programmed to record the number of attempts the child makes to log in, whether they are correct or not, and how long they spend on each page from when the page appears to when the child hits the login button. Figures 4.6, 4.7 and 4.8 show the sequences of accessing the different pages on the website for the different experimental sessions in the study.



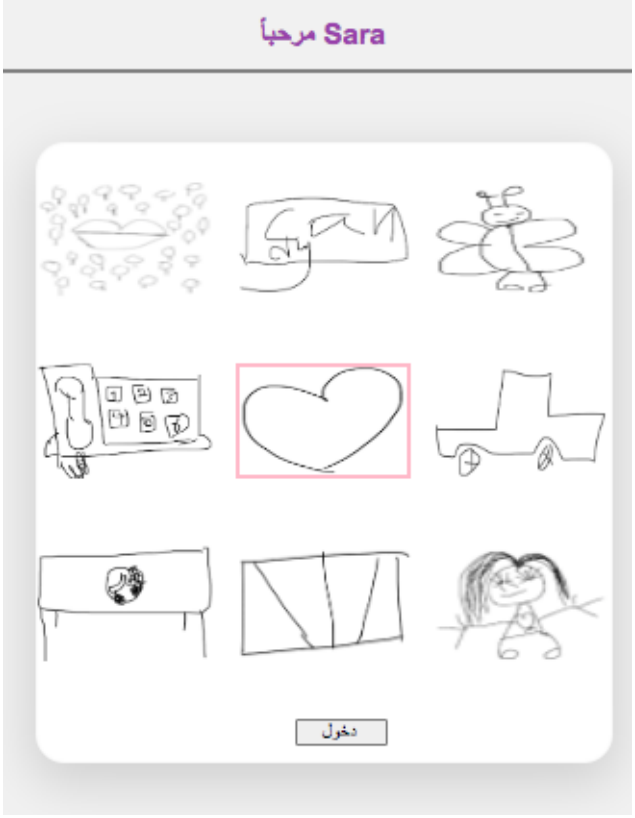
English version Username page

Arabic version Username page

Figure 5.3 Username page for the DoodlePass authentication system



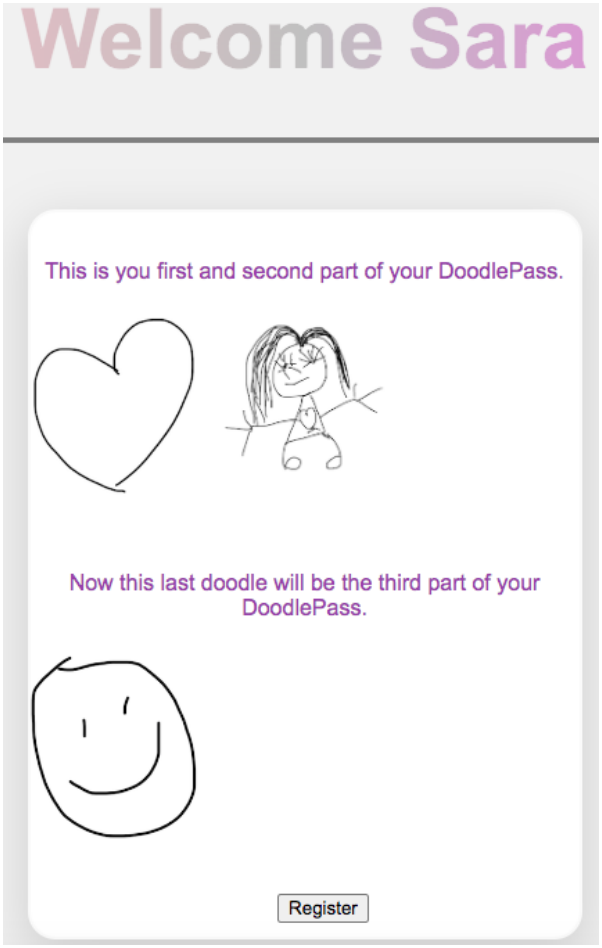
English version Login page



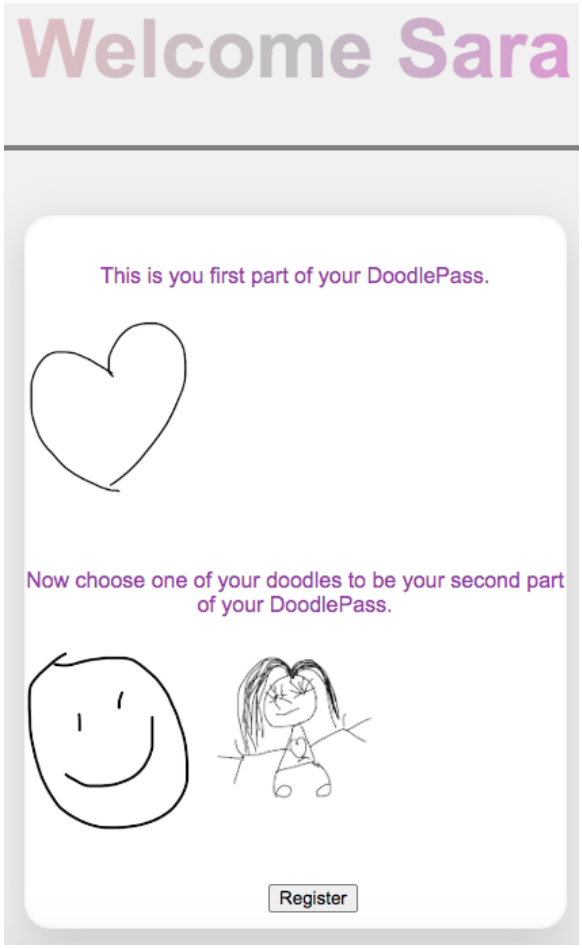
Arabic version Login page

Figure 5.4 Authentication grid of 3 x 3 doodles for the DoodlePass authentication system (login page)

Creating DoodlePass:1



Creating DoodlePass:2



Creating DoodlePass:3

Figure 5.5 Authentication key registration pages in DoodlePass authentication system

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 doodles were chosen to be in black and white to allow children to focus on drawing rather than choosing colours, to save time in the drawing session, and to avoid children being distracted at the authentication phase. Thus, this ensured the children recognise their doodles from their actual drawings and not from the colours.

A selection of games was made from the PBS Kids website (pbskids.org), appropriate for 6 to 12 year old children. Selected games were all educational and suitable for both girls and boys. In addition, some of these games had different levels or degree of difficulties, which made them suitable for playing for 10 minutes (see Appendix B.3).

Table 5.3 Open ended questions asked in each experimental session

Session	Questions
1	Questions asked at the beginning of the session: 1) Do you have any passwords? 2) Why do you think you need passwords? Questions asked at the end of the session: 3) Which do you think is easy to remember your text password or DoodlePass? 4) Which do you prefer more text password or DoodlePass?
2	Questions asked at the end of the session: 1) What type of digital devices do you use? 2) Do you use a password to access (each device from previous question)? 3) Do you have any password for online accounts?
3	No questions were asked during this session
4	Questions asked at the beginning of the session: 1) Do you think remembering three doodles for DoodlePass much harder than two doodles? 2) Do you think you would be able to remember three doodles as a DoodlePass for long time?
5	Questions asked at the beginning of the session: 1) Did you find it easy or hard to remember your DoodlePass? 2) How did you remember your DoodlePass? 3) Which one is easier to you to remember text password or DoodlePass? 4) Which one did you prefer more text password or DoodlePass?

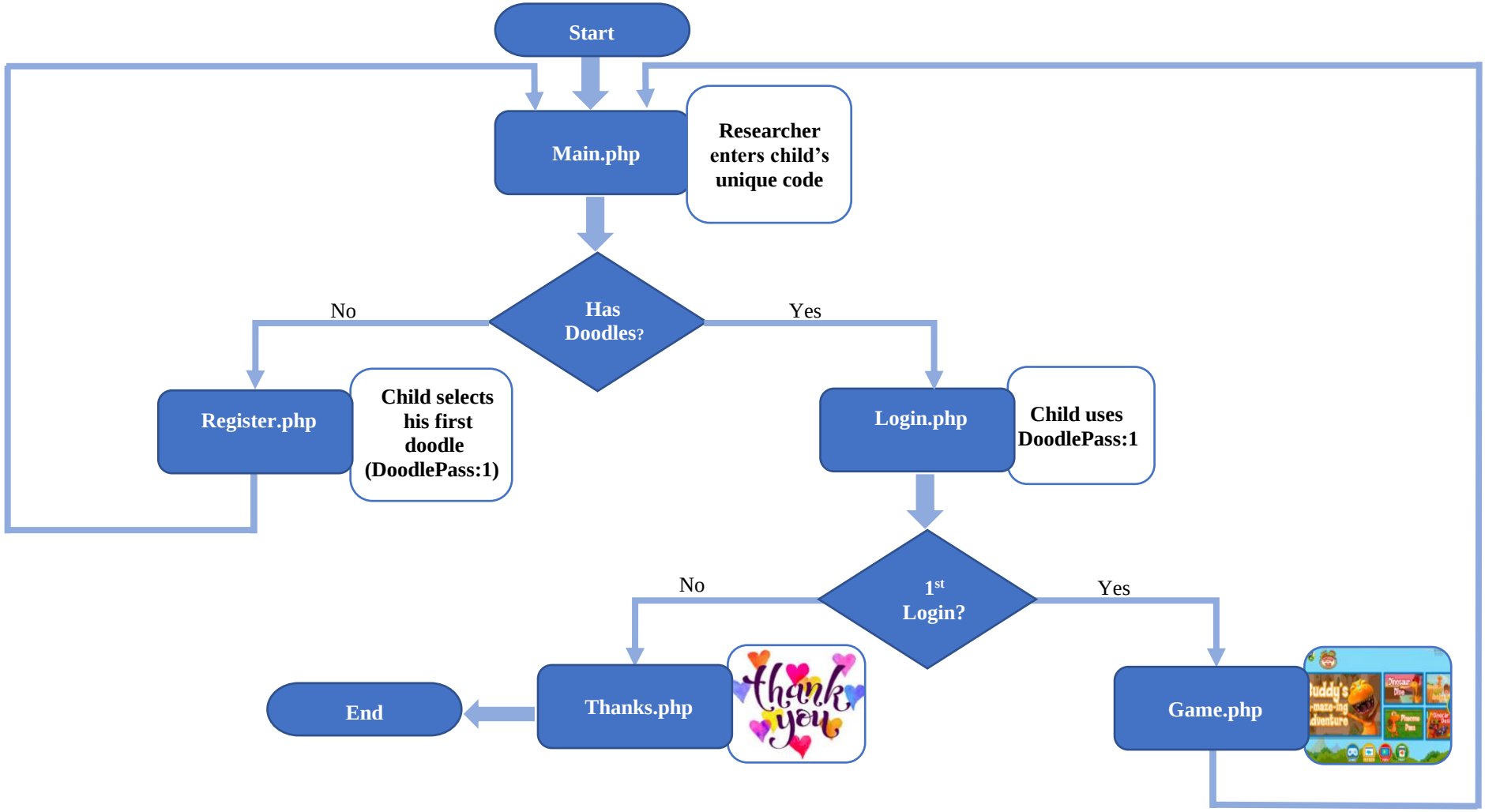


Figure 5.6 Website page sequences for the DoodlePass authentication system

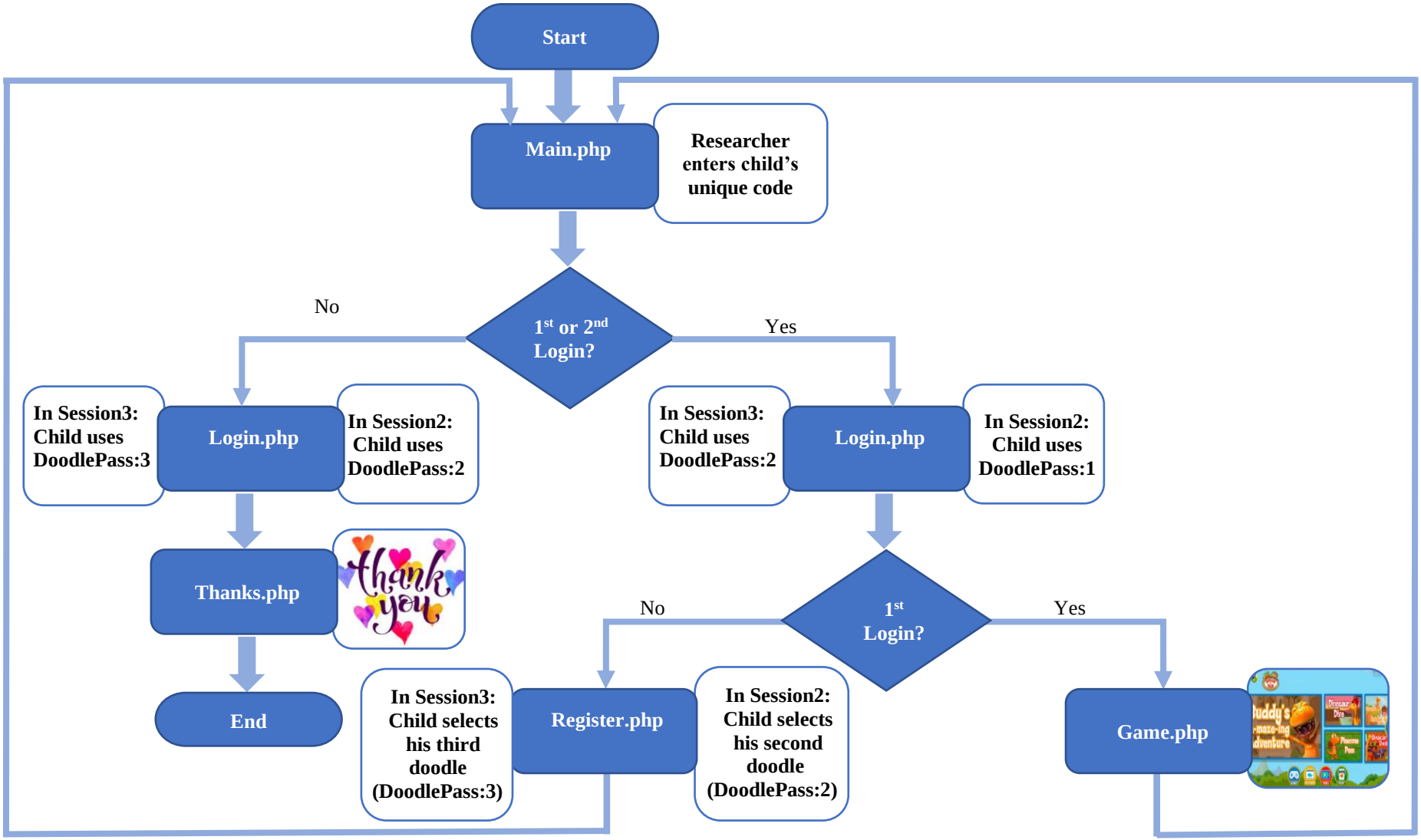


Figure 5.7 Website page sequences for Sessions 2 and 3 in the DoodlePass authentication system

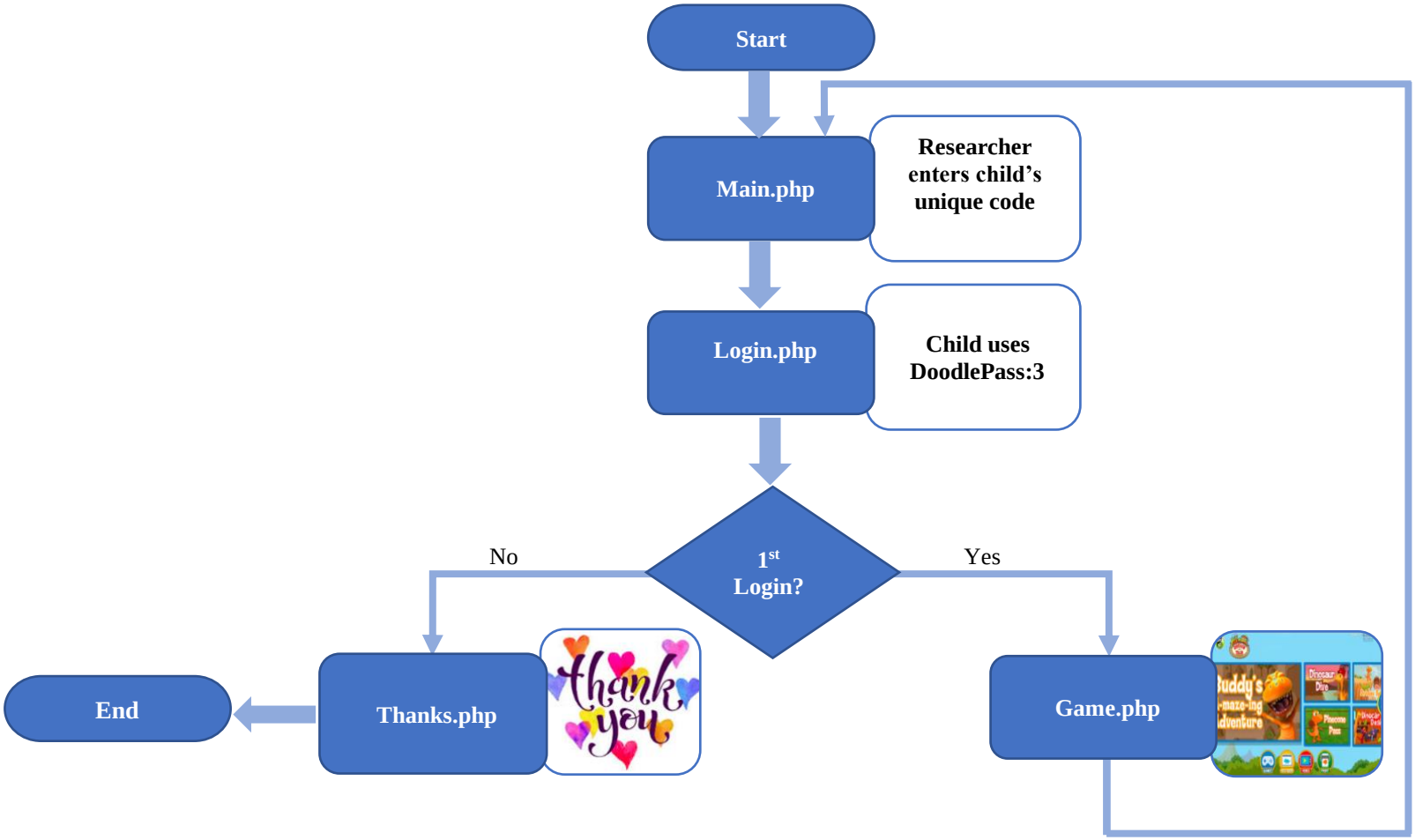


Figure 5.8 Website page sequences for Sessions 4 and 5 in the DoodlePass authentication system

5.2.4 Procedure

The study complied with the ethical research principles of the University of York. Permission was then sought from the Heads of the two schools in Riyadh, Saudi Arabia, the private international and the state-funded school, who sent letters to parents of children in Grades 1 to 6 (see Appendix B.2). Parents replied to the Head with a physical letter of consent if they were happy for their child to participate in the study. The schools gave permission for the children to take part in the study during their weekly art classes. I carried out the data collection at the private international school for all the girls, and the boys in Grades 1 to 3. Data collection for the state-funded school was undertaken by a teacher at that school for the boys in Grades 4 to 6 (as mentioned in section 1.2, there were no girls who participated at the state-funded school). The teacher was given a detailed protocol about how to conduct the sessions, and I also talked him through the procedure (see Appendix B.1). At each school, we were given a quiet room to meet the children and conduct the study.

At the beginning of the Pre-Session the children's verbal assent to participate in the research was sought. They were asked if they would help the researcher with their work which would involve creating an online account and logging in to that account a number of times. If they did so they would be able to play video games and receive a gift voucher at the end of the study. They were also told that they have the right to withdraw from the study any time, which also happened in Sessions 3, 4, and 5 (for more details, see Chapter 3, section 3.2.4).

They were then asked to draw three doodles on the iPad, all of different objects and on a different theme. They were told to draw simple doodles 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 DoodlePass grids with appropriate combinations of doodles (see section 4.2.5).

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 experimental session, the children were asked to select one of their three doodles as their DoodlePass and were told *"You need to identify your new doodle to get*

access to your account and play the game." They were then asked to log in to the games area. If they could not recognise their doodle from the 3 x 3 grid (see Figure 4.4), or chose an incorrect doodle, a friendly error message appeared: "*Oops! Something went wrong. Please try again*" (see Figure 4.9). The child was given three attempts at identifying their doodle then given a hint. If they had not identified their doodle after three attempts, an error message appeared contains researcher name: *"This is your 3rd attempt! Please ask [Esra] for a hint."* (see Figure 4.9). The researcher then 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 DoodlePass, an error message appeared: "*Oops! Something went wrong. Please ask [Esra] to tell you which one is your DoodlePass."* (see Figure 4.9), then the researcher showed them the correct one with the reassurance: "*It's OK, I will help you, but you need to try to remember it for next time*" This protocol of attempts, hints and assistance was followed for all logins throughout the study.

When the child had successfully logged in, they chose a video game to play for 10 minutes from the selection provided (see Appendix B.3). If the child started a game and did not like it (this happened very rarely), they were allowed to choose another game from the selection. Similarly, if they came to the end of the game before the 10 minutes was up, they could choose another game to play.

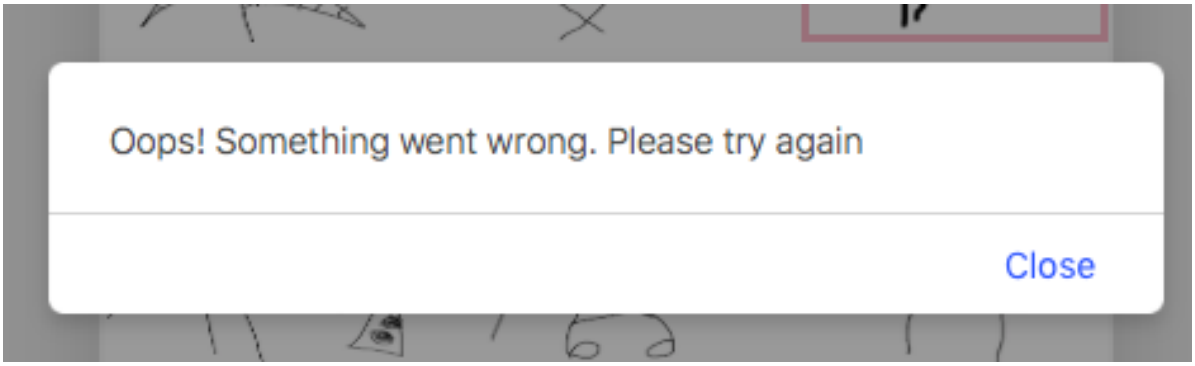
The child was then asked to log into the system again using their DoodlePass. In Session 1 they were told "*We want to ensure that you do not forget your DoodlePass to use it next week".* In Sessions 2 and 3 they were told: "*Now we need to make your DoodlePass stronger so we will choose a new doodle*". They were then taken to the registration page of the website to choose another doodle to add to their DoodlePass (see Figure 4.5).

At the time I was ready to do Session 5, the COVID-19 pandemic had started and lockdown was in effect in Saudi Arabia with all schools closed and no clear idea of when they would re-open. Therefore, due to these exceptional circumstances, Session 5 was done online and all participants with the other researcher withdraw from this study. I contacted each child separately through Zoom. Children had the option to participate using an audio-only or video call. I shared my screen with the child, and they told me which doodle is their DoodlePass. As it was not possible to play the video games over Zoom, they played a maze game with me, by

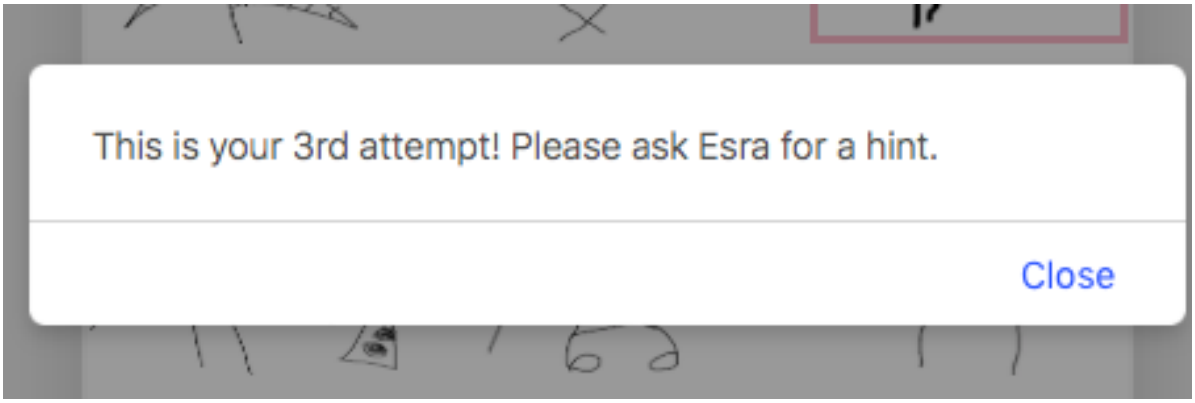
telling me (or drawing on the screen), the correct direction to reach the end of the maze. Thus, the times recorded in Session 5 are not comparable with the times in Sessions 1 to 4.

During each session, the children answered the questions related to the type of computer devices they use, their password usage and authentication mechanisms (see the schedule in Table 4.3).

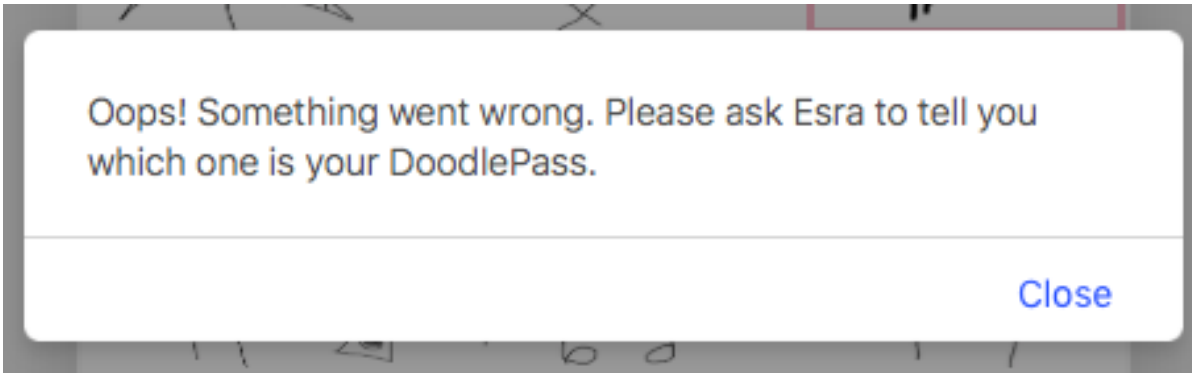
At the end of each session, they were thanked for their participation and told there would be another session in about a week's time, if appropriate. At the end of Session 4 they were thanked for their participation in the study, asked whether they had any questions about the study and given their gift voucher.



Error message appears in 1st and 2nd attempts



Error message appears in 3rd attempt



Error message appears in 4th attempt

Figure 5.9 Error messages in the DoodlePass authentication system

5.2.5 Data preparation and analysis

Data on a number of the quantitative variables from the study were not normally distributed, so non-parametric statistics were used. It is important to note that the time to login in this chapter is calculated based on the first successful attempt for each child This was in order to measure only child's best performance, but also to avoid time anomalies caused by a child's

errors or other problems e.g., technical issues, etc). Login times for each DoodlePass were investigated in depth for successive grades to see whether there were age differences between the children. Comparing all grades together against each other meant a great many comparisons and would have resulted in an unacceptably high Type I error rate (Lazar et al., 2010).

In some questions the effects of the children's age/grade were investigated. However, in some instances the number of children was small, so the children were grouped into levels of two grades (Grade 1 & 2, Grade 3 & 4, and Grade 5 & 6) (see Chapter 3, section 3.2.1 for more detail).

To analyse data for the open question a thematic analysis was used. The question was: How did you remember your DoodlePass? (Session 5, Q2).

The thematic analysis was conducted in a number of steps. First, my supervisor and I met and discussed an initial framework for the codes. Second, I conducted all the coding using these initial codes. Then I send it back to my supervisor who refine it to the final version. Third, we applied new codes to the participants' answers in two different version and then compare and agree on a final version.

In total 111 doodles were created by the children and were categorized before the first experimental session to allow creation of DoodlePass grids with appropriate combinations of doodles.

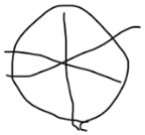
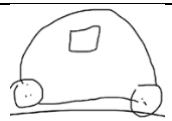
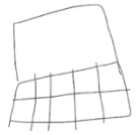
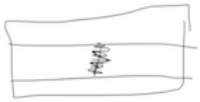
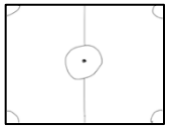
Categorisation of the doodles started with the children's own descriptions and then I refined the categories as needed. In some cases, doodles were categorized differently from the child's original description, as seen in Table 4.5. All categories contained two or more doodles drawn by children except for the Boat category, which contained only one doodle. Therefore, I drew one extra boat myself and added it, in order to have at least two doodles per category. In total, 27 different categories were created based on the children drawings (see Table 4.4).

In some cases, children struggled to draw either because they did not like drawing, or they tried to draw a complicated doodle. One of the children (a boy, Grade 3) thought that his ability to draw was not perfect and took a while until he was able to draw the three doodles. One particularly interesting instance was that another of the children (a girl, Grade 2) was angry with her drawing and took a very long time drawing. Then she erased the doodles she had

drawn, and she decided to draw a whole scene rather than individual doodles. I told her that I liked her drawings, but I would choose three objects from her drawing to be her doodles and she accepted that (see Figure 4.10).

With some of the other children, I realised that they drew things that were visible in the room where the study took place, such as a book, a laptop, a phone, etc. Examples include the book, the logo (which is the school's logo) and the mobile phone in Table 4.4.

Table 5.4 Categories of doodles with examples used in DoodlePass authentication system

Category	Count	Example	Category	Count	Example	Category	Count	Example
Animal	4		**Ball**	2		**Boat**	2	
Book	5		**Box**	9		**Boy**	9	
Candy	2		**Car**	6		**Computer**	2	
Doughnut	3		**Eye**	2		**Face**	4	
Flag	5		**Flower**	10		**Football Field**	2	

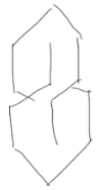
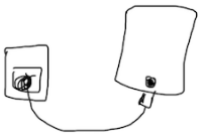
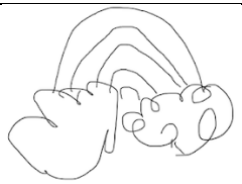
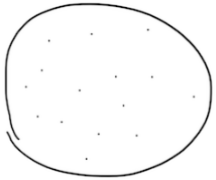
Category	Count	Example	Category	Count	Example	Category	Count	Example
Fruit	3		**Girl**	4		**Heart**	4	
House	9		**Letter**	2		**Logo**	4	
Mobile phone	3		**Mug**	5		**Rainbow**	2	
Star	2		**Sun**	3		**Tree**	4	

Table 5.5 Cases of doodle re-categorisation in DoodlePass authentication system

Case	Categorisation Refinement	Frequency of Occurrence	Example Case	Doodle	Child's Description for the Sample	Re- categorisation
Child drew two doodles which both fit in the same category	Check which one of the doodles can fit in another category	2	Child drew two type of fruits		Orange	doughnut
Child drew a doodle but could not give it a name	Check most suitable category for the doodle	3	Child drew randomly		Random	Logo
Child 's description of the doodle seemed similar to other children's doodles and could easily belong to the same category	Check most suitable category for the doodle	34	Child drew an ice cream		Ice cream	Heart

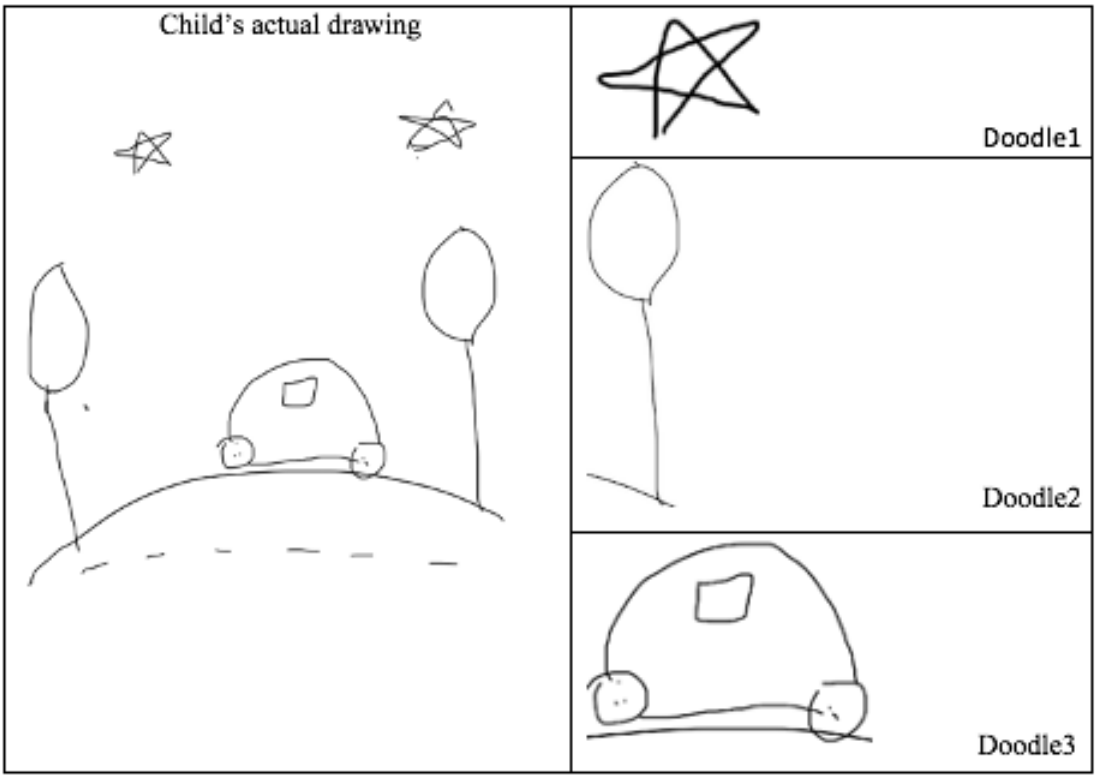


Figure 5.10 Complete drawing that I split into three doodles as the child chose not to draw individual doodles (see text in section 4.2.5)

5.3 Results

As part of this study was conducted during the COVID-19 pandemic, a number of participants withdrew and did not complete all sessions. Table 4.6 shows the number of participants who withdrew for each session for each grade of participants, none of these participants returned to the study.

Table 5.6 Number of participants who withdrew for each session about the DoodlePass authentication system

Grade	Initial Participants	Number of Participants Who Withdrew				
		Session 1	Session 2	Session 3	Session 4	Session 5
1	6 (3boys, 3girls)	0	0	0	0	1 girl
2	6 (3boys, 3girls)	0	0	0	0	2 girls
3	7 (4boys, 3girls)	0	0	0	0	0
4	5 (3boys, 2girls)	0	0	1 boy	4 (3boys, 1girl)	5 (3boys, 2girls)
5	7 (3boys, 4girls)	0	0	2 boys	3 boys	3 boys
6	6 (3boys, 3girls)	0	0	0	3 boys	4 (3boys, 1girl)
Total number of participants	37	37	37	34	27	22

The results in this chapter will be divided in to two parts; the first on the effectiveness (accuracy) and efficiency (time taken to login) of the DoodlePass authentication system; the second part on satisfaction with DoodlePass, particularly children's preferences for DoodlePass or a text password and which do they think is more memorable.

5.3.1 DoodlePass Authentication System

In this section the data that were collected from children while using DoodlePass authentication system is analysed separately for each authentication key of DoodlePass. Thus, in this section when I refer to DoodlePass:1, it means authentication with the first doodle that the children created in the Pre-Session. DoodlePass:2 refers authentication with both the first doodle and the second doodle that children created in the Pre-Session. DoodlePass:3 refers to authentication with all three doodles that children created.

5.3.1.1 DoodlePass:1

All 37 participants were able to login using their DoodlePass:1. Table 4.7 shows the accuracy (selection of the correct Doodle on the first or subsequent attempts) and median times for successful first attempts (with semi interquartile ranges) for DoodlePass:1, across the four presentations of DoodlePass:1 in Sessions 1 and 2. These median times are also illustrated in Figure 4.11.

Table 5.7 Accuracy and median times for login with DoodlePass:1

Session	Login Number	Login Accuracy	Median Login Time (Successful 1st Attempts)	SIQR
1	1	37/37 on 1st attempt (100%)	9.59	1.72
	2	35/37 on 1st attempt (94.59%) 2/37 on 2nd attempt (5.4%)	7.58	1.75
2	1	36/37 on 1st attempt (97.3%) 1/37 on 2nd attempt (2.7%)	8.03	3.54
	2	33/37 on 1st attempt (89.2%) 3/37 on 2nd attempt (8.1%) 1/37 on 4th attempt (2.7%)	7.45	2.86

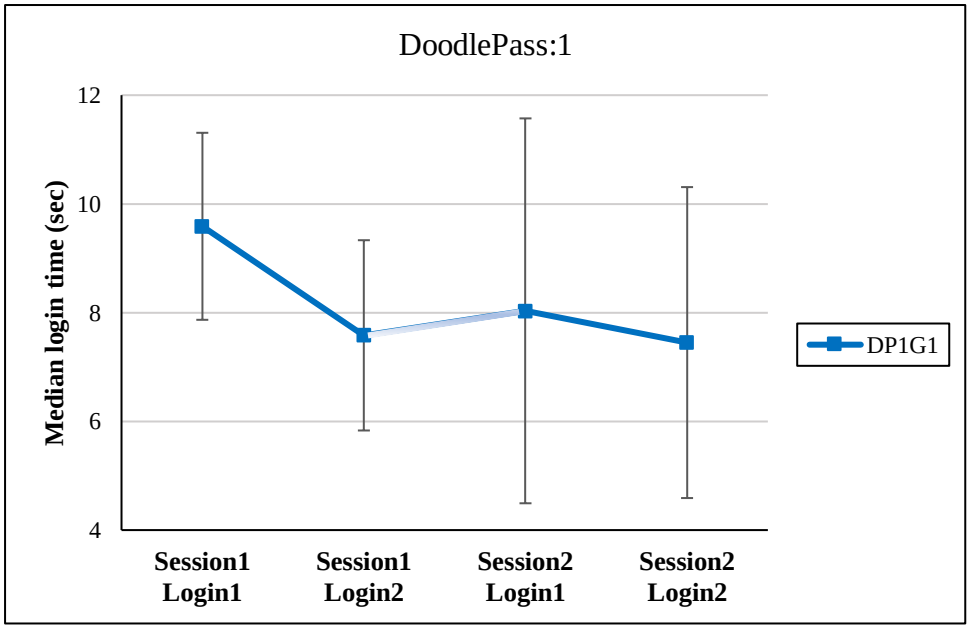


Figure 5.11 Median times and semi interquartile ranges for successful first logins for DoodlePass:1
Note: Shaded line indicates the one week gap between Session 1 and Session 2

The accuracy figures in Table 4.7 show that almost all the children were able to recognise their DoodlePass:1 on all occasions. On only a small number of occasions did children need a second or on one occasion a fourth attempt (7 occasions out of a total of 148, so 4.73% in all; 6 from the second attempt and one from the fourth attempt). With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the times to login with DoodlePass:1 on the different login occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed no significant difference between the four logins, FM = 4.76, df = 3, p = 0.19. A related samples Wilcoxon tests were also conducted between the login times for the two logins in Session 1 and the two logins in Session 2, to investigate whether participants became faster on a second login within the one session. These showed a significant decrease from the 1st login to the 2nd login in Session 1 (W = -2.85, p = 0.004), but no significant difference between logins in Session 2 (W = 0.67, p = 0.50). A related samples Wilcoxon test was also conducted on the login times for the 2nd login in Session 1 and in 1st login in Session 2 to investigate whether times were longer after a one week break. This showed no significant difference between these two logins (W = -1.50, p = 0.14). However, as Table 4.7 and Figure 4.11 show, the interquartile range for Session 2, Login 1 is the longest of the four logins. This shows that at this login some participants recognised and selected their DoodlePass:1 quickly while others took a considerably longer time, and this might be due to the one week gap between Sessions 1 and 2.

To investigate whether there were age differences between the children in the login times for DoodlePass:1, independent samples Kruskal-Wallis tests were conducted between the 1st to 6th grade groups on the times for each login. The results are summarised in Table 4.8. This shows that there were significant grade differences at Session 1, Login 2 and Session 2, Login 1. To establish exactly where the differences between the grades lay, a series of Mann-Whitney tests was conducted between the login times for successive grades for these two logins.

Table 5.8 Kruskal-Wallis tests of grade differences in DoodlePass:1 login times

Session	Login	Number of Participants with Successful 1st Attempts	Kruskal-Wallis Observed Value	df	p
1	1	37/37	6.16	5	0.29
	2	35/37	12.73	5	0.03
2	1	36/37	14.28	5	0.01
	2	33/37	8.59	5	0.13

Figure 4.12 shows the median login times for Session 1, Login 2 for each grade of participants and Table 4.9 shows the results of the Mann-Whitney tests on successive grades. Figure 4.12 suggests that there an increase in times in Grade 5 and 6 with significant increases from Grade 4 to 5 and Grade 5 to 6 (see Table 4.9). Overall, when Grade 1 is compared with Grade 6, there is no significant difference in login time (U = - 0.91, p = 0.44).

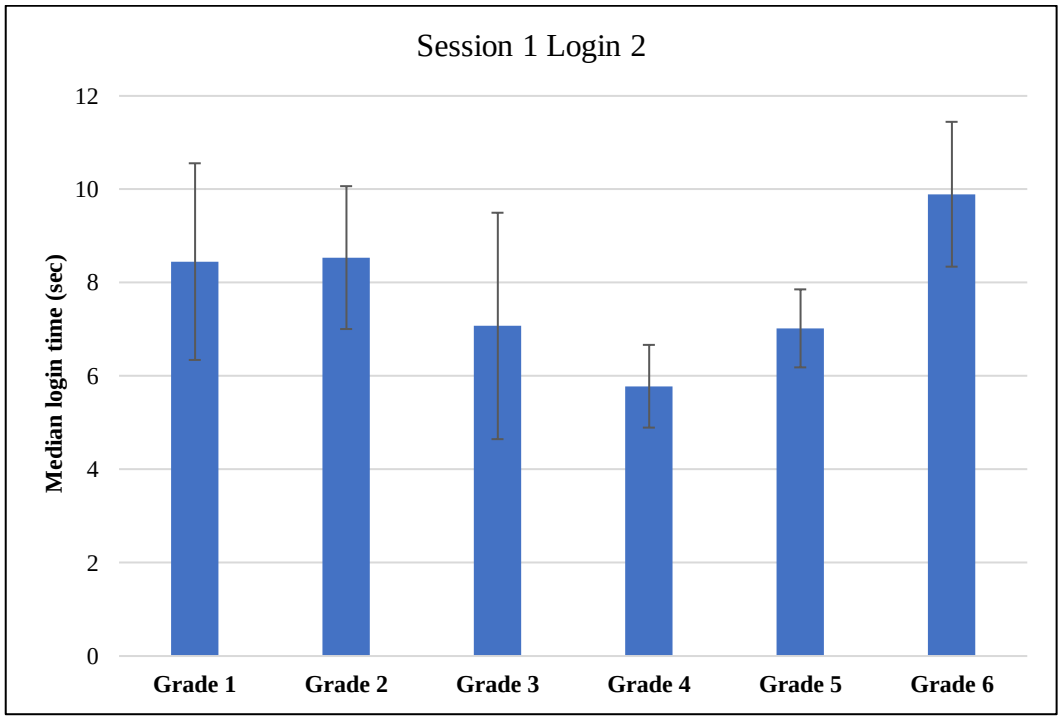


Figure 5.12 Median times for successful first logins for DoodlePass:1 for Session 1, Login 2 for children in each grade

Table 5.9 Mann-Whitney tests of differences between grades in DoodlePass:1 login times for Session 1, Login 2 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	8.5	2.1		
2	8.5	1.5	-0.18	0.93
3	7.1	2.4	-1.12	0.31
4	5.8	0.9	-1.64	0.13
5	7.0	0.8	2.52	0.01
6	9.9	1.6	2.00	0.05

For Session 2, Login 1, Figure 4.13 shows the median login times for each grade of children and Table 4.10 show the results of the Mann-Whitney tests on successive grades. Figure 4.13 shows a similar pattern to Session 1, Login 2, with apparently decreasing times from Grades 1 to 5, but then an apparent increase in times in Grade 6. However, Table 4.10 shows there are no significant differences between successive grades. On the other hand, when Grade 1 is compared with Grade 6, there is a significant decrease in login time (U = -2.37, p = 0.02).

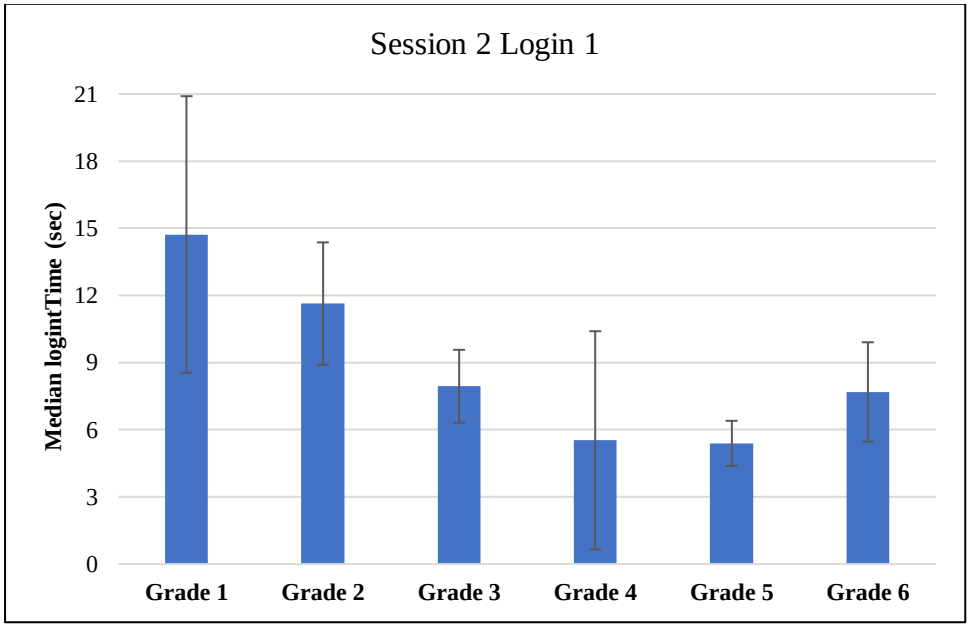


Figure 5.13 Median times for successful first logins for DoodlePass:1 for Session 2, Login 1 for children in each grade

Table 5.10 Mann-Whitney tests of differences between grades in DoodlePass:1 login times for Session 2, Login1 (each grade compared to the previous grade)

Grade	Median login time	SIQR	Mann-Whitney (U)	p
1	14.7	6.2		
2	11.6	2.7	-1.10	0.33
3	7.9	1.6	-1.14	0.30
4	5.5	4.9	-0.89	0.43
5	5.4	1.0	-0.57	0.64
6	7.7	2.2	1.43	0.18

5.3.1.2 DoodlePass:2

37 participants took part in Session 2 when DoodlePass:2 was introduced. However, before Session 3, 3 participants withdrew, leaving 34 participants, as shown in Table 4.11.

All 37 participants were able to login using of DoodlePass:2 (Session 3, Login 3). Table 4.12 shows the accuracy of recognising and selecting the correct doodle (on the first and subsequent attempts) for each of the two grids of doodles in DoodlePass:2 and median times for successful first login attempts (with semi interquartile ranges) for each grid. These median times are also illustrated in Figure 4.14.

Table 5.11 Number of participants in DoodlePass:2 sessions

Session	Login	Overall Number of Participants
2	3	37
3	1	34
	2	34

Table 5.12 Accuracy and median times for login with DoodlePass:2

Session	Login Number	Login Accuracy	Median Login Time (Successful 1st Attempts)	SIQR
2	3	Grid1: 35/37 on 1st attempt (94.6%) 2/37 on 2nd attempt (5.4%)	8.50	3.88
		Grid2: 37/37 on 1st attempt (100%)	7.37	2.76
3	1	Grid1: 32/34 on 1st attempt (94.1%) 1/34 on 2nd attempt (2.9%) 1/34 on 3rd attempt (2.9%)	9.13	3.42
		Grid2: 33/34 on 1st attempt (97.1%) 1/34 on 2nd attempt (2.9%)	8.01	2.71
	2	Grid1: 33/34 on 1st attempt (97.1%) 1/34 on 3rd attempt (2.9%)	8.17	3.06
		Grid2: 32/34 on 1st attempt (94.1%) 2/34 on 2nd attempt (5.9%)	7.82	2.56

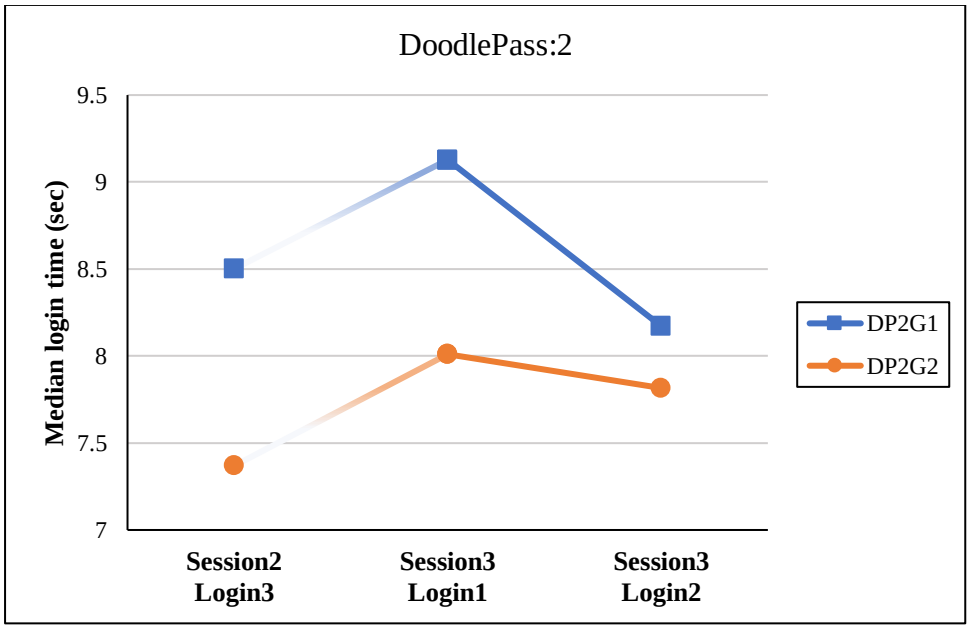


Figure 5.14 Median times for Session 2 and Session 3 logins for DoodlePass:2

Note: DP2G1: DoodlePass2, Grid 1; DP2G2: DoodlePass2, Grid 2; Shaded lines indicates the one week gap between Session 2 and Session 3.

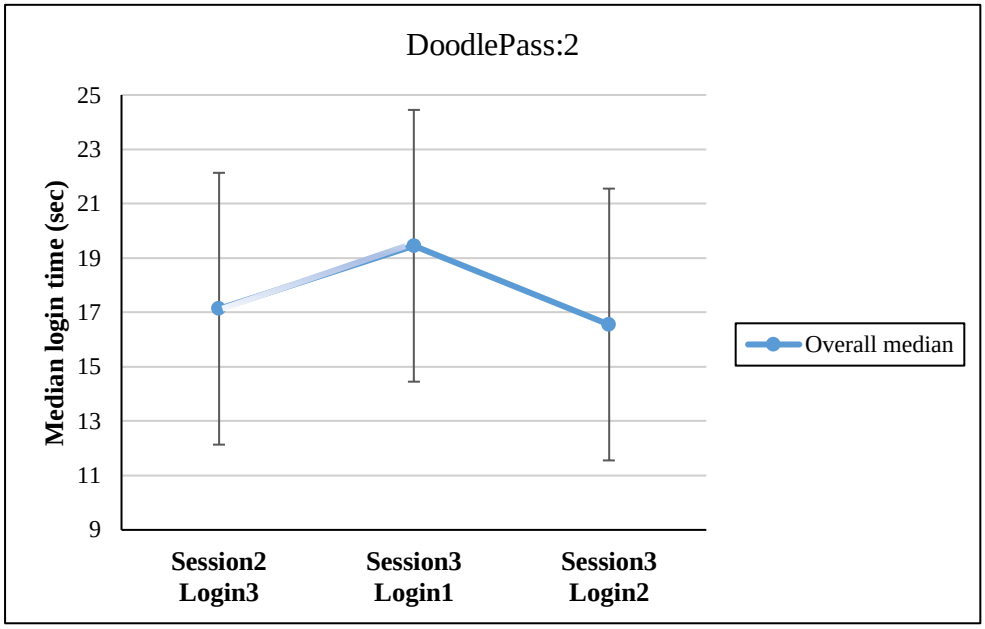


Figure 5.15 Overall median times and semi interquartile ranges for DoodlePass:2

The accuracy figures in Table 4.12 show that children were in general very accurate in recognising and selecting the correct doodles for DoodlePass:2. On only a small number of occasions did children need a second or third attempt (on 8 occasions out of a total of 210, so on 3.8% of occasions; 6 occasions on the second attempt and 2 occasions on the third attempt). Two children (one child in Grade 4: Session 3, Login 1; one child in Grade 3: Session 3, Login 2) needed a third attempt to recognise their DoodlePass:2, one week after they had created and used the DoodlePass:2 for the first time. With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the differences in the overall login times which were successful at the first attempt on the different login occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed no significant difference between the three logins, FM = 5.21, df = 2, p = 0.07. In addition, related samples Wilcoxon tests were conducted between the different logins: the login times for the 3rd login in Session 2 and 1st login in Session 3, as well as between the 1st and 2nd login in Session 3. There was no significant difference between the 3rd login in Session 2 and the 1st login in Session 3 (W = 0.50, p = 0.55), but a significant decrease from the 1st login to the 2nd login in Session 3 (W = -1.52, p = 0.13). The semi interquartile ranges, as shown in Figure 4.15, are large for all these logins, suggesting that some

children quickly recognised and selected their DoodlePass:2 while others took a much longer time.

To investigate whether there were age differences in the login times for DoodlePass:2, independent samples Kruskal-Wallis tests were conducted on the overall login times (i.e., the sum of the time to select the correct doodle from the first grid and the time to select the correct doodle from the second grid which were successful at the first attempt for each grid) for each login for children in the different grades. The results are summarised in Table 4.13. This shows that there are significant grade differences at all three logins. To establish exactly where the differences between the grades lay, a series of Mann-Whitney tests was conducted between the login times for successive grades for these logins.

Table 5.13 Kruskal-Wallis tests of grade differences in overall DoodlePass:2 login times

Session	Login	Number of Participants with Successful 1st Attempt on all Grids	Kruskal-Wallis Observed Value	df	p
2	3	35/37	19.80	5	0.001
3	1	31/34	10.88	5	0.05
	2	31/34	14.02	5	0.02

For Session 2, Login 3, Figure 4.16 shows the overall median login times for each grade of children and Table 4.14 show the results of the Mann-Whitney tests on successive grades. Figure 4.16 shows that the trend in times is generally to faster times as the children get older. However, there are no significant decreases from Grades 1 to 3, but then a significant decrease from Grade 3 to 4, and no further significant decrease after that. When we compare Grade 1 with Grade 6, there is a significant decrease in overall login time ($U = -2.24$, $p = 0.03$).

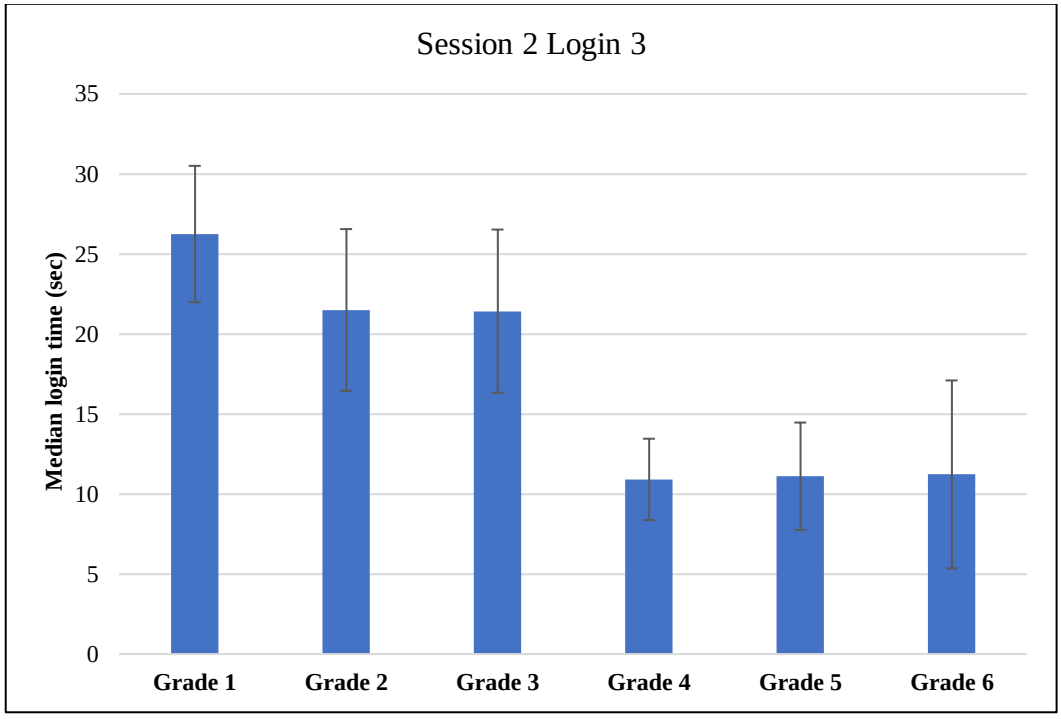


Figure 5.16 Median times for successful first logins for DoodlePass:2 for Session 2, Login 3 for children in each grade

Table 5.14 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 2, Login 3 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	26.2	4.3		
2	21.5	5.1	-0.80	0.49
3	21.4	5.1	-0.48	0.70
4	10.9	2.5	-2.74	0.004
5	11.1	3.4	-0.18	0.93
6	11.2	5.9	-0.64	0.59

For Session 3, Login 1, Figure 4.17 shows the median overall login times for each grade of children and Table 4.15 show the results of the Mann-Whitney tests on successive grades. Figure 4.17 shows that the overall trend is for faster login times as the children get older, although the decreases are not consistent. This is reinforced by Table 4.15, which shows there are no significant differences between successive grades. However, when Grade 1 is compared with Grade 6, there is a significant decrease in login time (U = - 2.08, p = 0.04).

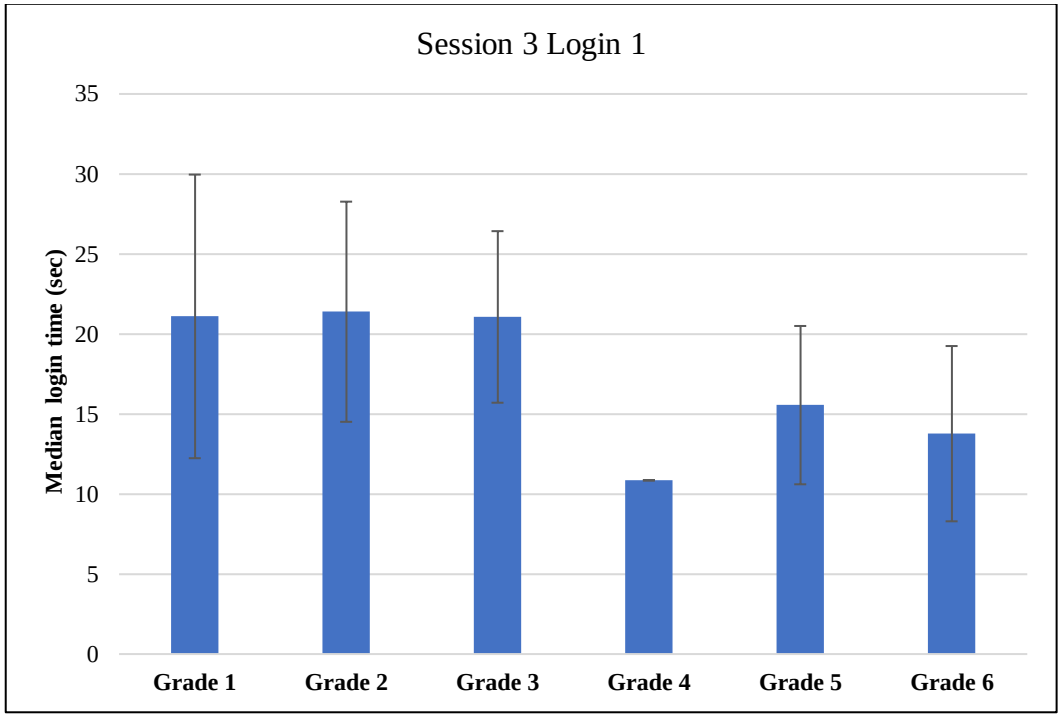


Figure 5.17 Median times for successful first logins for DoodlePass:2 for Session 3, Login 1 for children in each grade (no SIQR for grade 4 as only two values)

Table 5.15 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 3, Login1 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	21.1	8.9		
2	21.4	6.9	-0.32	0.82
3	21.1	5.4	-0.48	0.70
4	10.9	no value*	-2.00	0.07
5	15.6	4.9	-1.16	0.38
6	13.8	5.5	-0.55	0.66

* There were only 2 children in Grade 4, SIQR cannot be calculated for less than 5 values.

For Session 3, Login 2, Figure 4.18 shows the overall median login times for each grade of children and Table 4.16 show the results of the Mann-Whitney tests on successive grades. Figure 4.18 shows that the trend in times is generally to faster times as the children get older. However, Table 4.16, shows that there are no significant differences between successive grades. But when Grade 1 is compared with Grade 6, there is a significant decrease in login time (U = -2.24, p = 0.03).

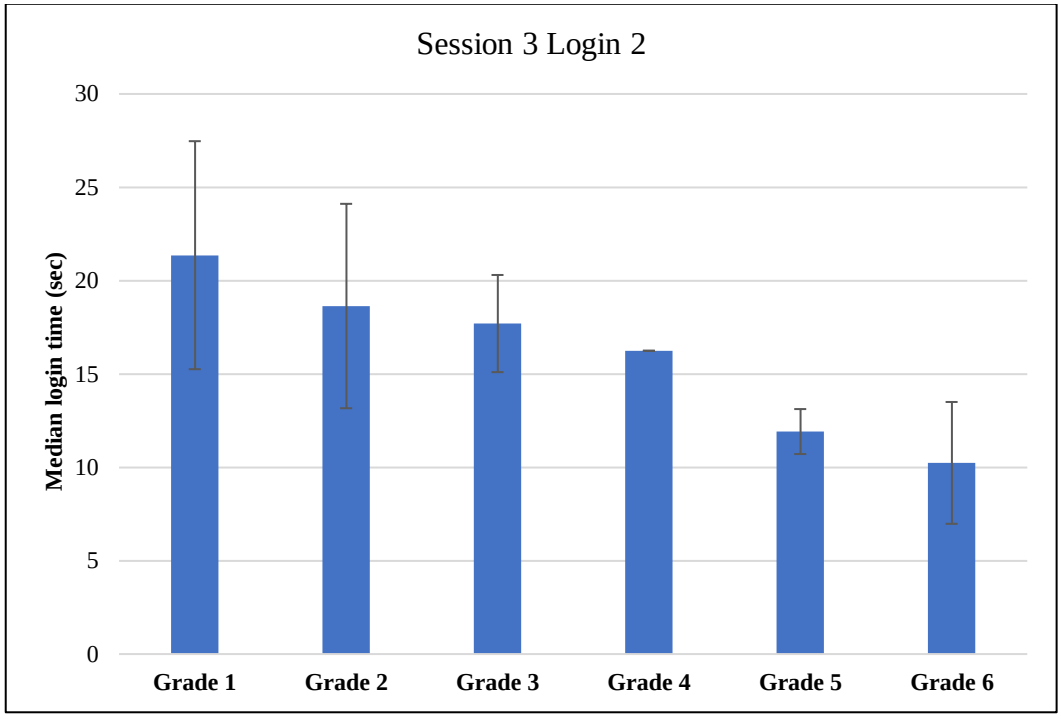


Figure 5.18 Median times for successful first logins for DoodlePass:2 for Session 3, Login 2 for children in each grade (no SIQR for grade 4 as only four values)

Table 5.16 Mann-Whitney tests of differences between grades in DoodlePass:2 login times for Session 3, Login2 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	21.4	6.1		
2	18.6	5.5	-0.64	0.59
3	17.7	2.6	-0.37	0.79
4	16.2	no value*	-0.75	0.57
5	11.9	1.2	-0.75	0.75
6	10.2	3.3	-1.10	0.33

* There were only 4 children in Grade 4, SPSS cannot calculate SIQR for less than 5 values.

5.3.1.3 DoodlePass:3

34 participants completed choosing their DoodlePass:3 on the first trial, Session 3, Login 3. However, in Session 4, 7 participants withdrew, leaving 27 participants. In Session 5 (which was 9 months later), 5 more participants withdrew, leaving 22 participants (see Table 4.17). Table 4.18 shows the accuracy (selection of the correct doodles on the first attempt or subsequent attempts) and median times for successful first attempts (with semi interquartile ranges) to recognise and select the doodles for DoodlePass:3. These median times are also

illustrated in Figure 4.19. Figure 4.19 shows a jump from Session 3, Login 3 to Session 4, Login 1. This is due to the one week gap. Then there is another jump from Session 4, Login 2 to Session 5, Login 1, as a result of the approximately nine month gap.

Table 5.17 Number of participants in DoodlePass:3 sessions

Session	Login	Overall Number of Participants
3	3	34
4	1	27
	2	27
5	1	22
	2	21

Table 5.18 Accuracy and median times for login with DoodlePass:3

Session	Login Number	Login Accuracy	Median Login Time (successful 1st attempts)	SIQR
3	3	Grid1: 34/34 on 1st attempt (100%)	6.99	2.52
		Grid2: 32/34 on 1st attempt (94.1%) 1/34 on 2nd attempt (2.9%) 1/34 on 3rd attempt (2.9%)	6.80	2.68
		Grid3: 33/34 on 1st attempt (97.1%) 1/34 on 2nd attempt (2.9%)	6.38	2.03
4	1	Grid1: 26/27 on 1st attempt (96.3%) 1/27 on 2nd attempt (3.7%)	9.27	3.41
		Grid2: 26/27 on 1st attempt (96.3%) 1/27 on 2nd attempt (3.7%)	9.92	2.68
		Grid3: 26/27 on 1st attempt (88.9%) 3/27 on 2nd attempt (11.1%)	8.13	2.52
	2	Grid1: 26/27 on 1st attempt (96.3%) 1/27 on 2nd attempt (3.7%)	6.45	1.23
		Grid2: 25/27 on 1st attempt (92.6%) 2/27 on 2nd attempt (7.4%)	7.16	1.68
		Grid3: 26/27 on 1st attempt (96.3%) 1/27 on 4th attempt (3.7%)	6.24	1.67

5	1	Grid1: 13/22 on 1st attempt (59.1%) 7/22 on 2nd attempt (31.8%) 1/22 on 3rd attempt (4.5%) 1/22 on 4th attempt (4.5%)	12.96	7.08
		Grid2: 15/22 on 1st attempt (68.2%) 4/22 on 2nd attempt (18.2%) 2/22 on 3rd attempt (9.1%) 1/22 on 4th attempt (4.5%)	13.01	4.24
		Grid3: 15/22 on 1st attempt (68.2%) 2/22 on 2nd attempt (9.1%) 1/22 on 3rd attempt (4.5%) 2/22 on 4th attempt (9.1%) 2/22 on 5th attempt (9.1%)	15.22	4.14
	2	Grid1: 14/21 on 1st attempt (66.7%) 6/21 on 2nd attempt (28.6%) 1/21 on 3rd attempt (4.8%)	8.30	2.44
		Grid2: 19/21 on 1st attempt (90.5%) 1/21 on 2nd attempt (4.8%) 1/21 on 4th attempt (4.8%)	9.60	2.77
		Grid3: 17/21 on 1st attempt (81%) 2/21 on 2nd attempt (9.5%) 1/21 on 4th attempt (4.8%) 1/21 on 5th attempt (4.8%)	7.05	1.82

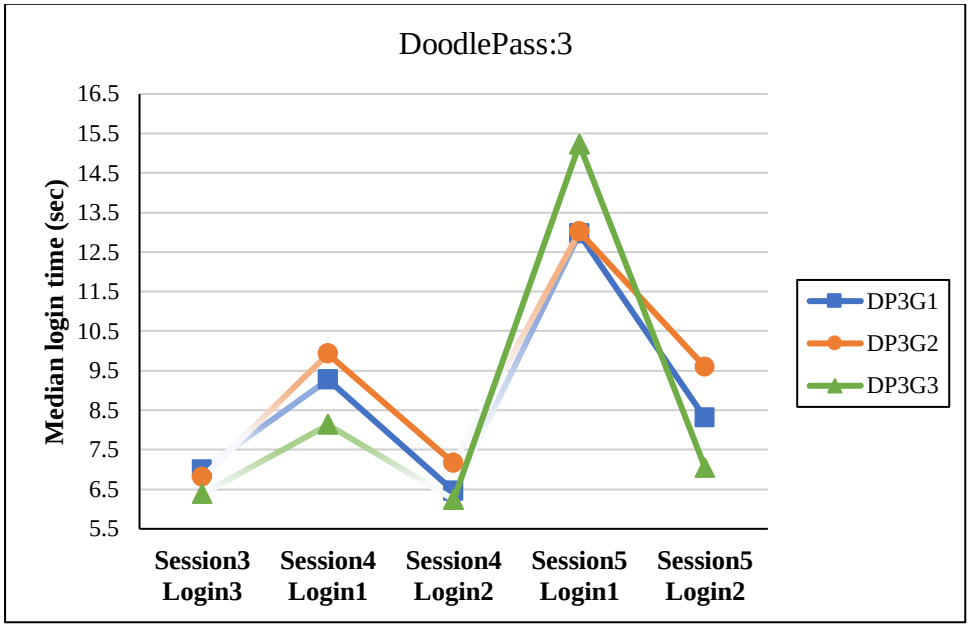


Figure 5.19 Median times for Session 3, Session 4, and Session 5 logins for DoodlePass:3

Notes: (1) DP3G1: DoodlePass3 Grid 1, DP3G2: DoodlePass3 Grid 2, DP3G3: DoodlePass3 Grid3.
(2) Shaded line indicates the one week gap between Sessions 3 and 4 and the approx. nine month gap between Sessions 4 and 5.

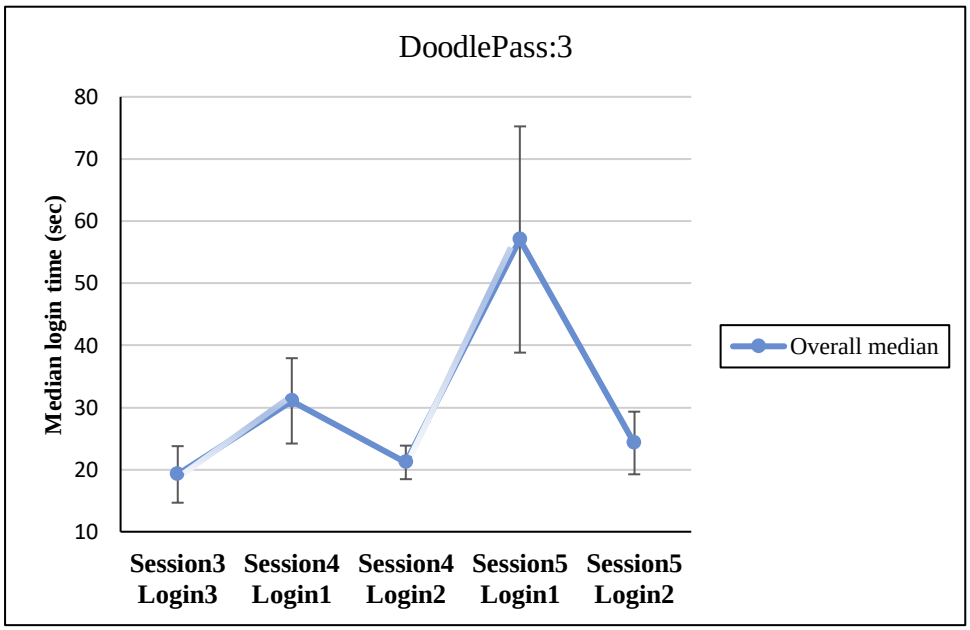


Figure 5.20 Overall median times and semi interquartile ranges for DoodlePass:3

The accuracy figures in Table 4.18 show that most of the children were able to remember their DoodlePass:3 on all occasions. On only a small number of occasions did children need more than one attempt, except in Session 5. On 48 occasions out of a total of 393 children needed more than one attempt, so on 12.2% of trials overall. This included 32 occasions on the second attempt, 6 on the third attempt, 7 on the fourth attempt, and 3 on the fifth attempt. However, for Session 5 which was 9 months after Session 4, more than 60% of children needed a second attempt. This included 5 children who needed a third attempt, 4 children who needed a fourth attempt, and 3 children who needed a fifth attempt. So over nine months after they had created and used the DoodlePass:3, recognition rates were still high and it seems that as children got into the task they remembered more. With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the overall times to login to DoodlePass:3 on the different occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. However, only two children remembered their DoodlePass:3 on the first attempt in all logins, therefore, no inferential analysis could be undertaken. This is expected due to the long period (9 months) between first three logins and last two logins. Instead, a related samples Friedman's two way analysis of variance by ranks was conducted with 17 participants who were successful on their first attempts for the first three logins (Session 3, Login 3 and Session 4, Login 1 and 2). This test showed no significant difference between the three logins, FM = 5.6, df = 2, p = 0.06. Additionally, related samples Wilcoxon tests were between successive logins both within and between Sessions 3, 4 and 5. Table 4.19 shows that there was significant increase between Session 3 and Session 4 (approximately one week apart). In the case of the comparison within Session 4 (Login 1 and Login 2) there was a significant decrease. Between Session 4 and Session 5 (approximately nine months apart) there was a significant increase in overall login time. Going back to Figure 4.20, it is interesting that semi interquartile range for Session 5, Login 1 is greater than the other logins, which suggests that some children in this session could remember their DoodlPass:3 quickly while others took longer time, and this is probably due to the 9 months gap between Sessions 4 and 5.

Table 5.19 Wilcoxon tests of differences in overall login times between successive logins for DoodlePass:3

Login	Number of Participants Successful on 1st Attempt on all Grids	Related Sample Wilcoxon Test	p
Session 3, Login 3 & Session 4, Login 1	20	-2.28	0.02
Session 4, Login 1 & Session 4, Login 2	18	-2.37	0.02
Session 4, Login 2 & Session 5, Login 1	5	-2.02	0.04

* For Session 5 there were only 4 children remembered their DoodlePass:3 on the first attempt in all logins, therefore, no inferential analysis was undertaken between Session 5.

To investigate whether there were age differences in the login times for DoodlePass:3, independent samples Kruskal-Wallis tests were conducted on the times for each login. The results are summarised in Table 4.20. There was a significant difference only on Session 3, Login 3.

Table 5.20 Kruskal-Wallis tests of grade differences in overall DoodletPass:3 login times

Session	Login	Number of Participants with Successful 1st Attempt on all Grids	Kruskal-Wallis Observed Value	df	p
3	3	31/34	12.62	5	0.03
4	1	22/27	7.49	5	0.19
	2	23/27	9.31	5	0.10
5	1	7/22	2.43	5	0.49
	2	1/21	8.46	5	0.08

For Session 3, Login 3, Figure 4.21 shows the overall median login times for each grade of children and Table 4.21 show the results of the Mann-Whitney tests on successive grades. Figure 4.21 shows that the trend in times is generally to faster times as the children get older, but there is an increase as well as a decrease in the pattern. This is reinforced by Table 4.21, which shows there are no significant differences between successive grades. However, when Grade 1 is compared with Grade 6, there is a significant decrease in login time (U = -1.98, p = 0.05).

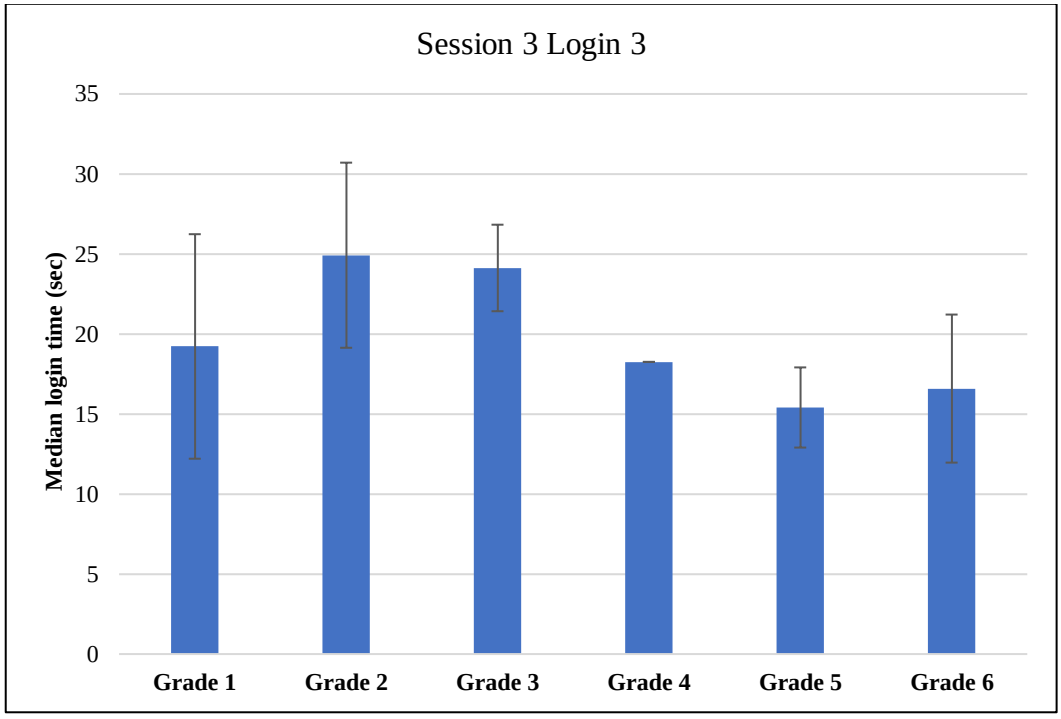


Figure 5.21 Median times for successful first logins for DoodlePass:3 for Session 3, Login 3 for children in each grade (no SIQR for grade 4 as only two values)

Table 5.21 Mann-Whitney tests of differences between grades in DoodlePass:3 login times for Session 3, Login 3 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	19.2	7.0		
2	24.9	5.8	-0.73	0.54
3	24.1	2.7	-1.14	0.30
4	18.3	no value*	-0.57	0.67
5	15.4	2.5	-1.94	0.07
6	16.6	4.6	-0.31	0.84

* There were only 2 children in Grade 4, SIQR cannot be calculated for less than 5 values.

Table 4.22 shows number of children who have more than one attempt for each grade of children. The results in this table show that the number of attempts decreases dramatically with the age of children, and this could be due to children's developing cognitive abilities. It is also interesting to notice that only younger children in Grade 1-3 have 4 and 5 attempts and need help to recognize and select their doodles.

Table 5.22 Number of children who have more than one attempt while using DoodlePass:3 authentication system for each grade

Number of Attempts	Grade 1	Grade 2	Grade 3	Grade 4	Grade 5	Grade 6
2	15	3	14	3	7	2
3	1	2	1	1	2	1
4	2	3	3	0	0	0
5	1	2	0	0	0	0
Total	19 (30.2%)	10 (15.9%)	18 (28.6%)	4 (6.3%)	9 (14.3%)	3 (4.8%)

5.3.2 Children's preferences between DoodlePass and a text password and memorability issues related to DoodlePass

In Session 1, the children were asked whether they thought remembering DoodlePass or a text password would be easier (Q3). All of the 37 participants answered this question. 67.6% of children said they thought DoodlePass would be easier to remember, 27% of children said they thought text password would be easier, and only (5.4%) of children said both. A chi-square test showed that there was a significant tendency to think that the DoodlePass would be easier to remember (comparing all three options: chi-square = 22.1, df = 2, $p < 0.000$; comparing only text password and DoodlePass: chi-square = 6.43, df = 1, p = 0.01). Table 4.23 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 3.46, df = 4, p= 0.48; comparing only text password and DoodlePass: chi-square = 2.44, df = 2, p= 0.29).

Table 5.23 Breakdown of preference for DoodlePass and text password for ease of remembering by children's grade (N = 37)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
DoodlePass	10	6	9	25
	83.3%	50%	69.2%	67.6%
Text password	2	5	3	10
	16.7%	41.7%	23.1%	27%
equally easy	0	1	1	2
	0.0%	8.3%	7.7%	5.4%

Children were asked another question in Session 1 as whether they prefer DoodlePass or text password (Q4). All of the 37 participants answered this question. Interestingly, four children who said DoodlePass was easier to remember than a text password said they preferred a text password to DoodlePass, and one child who said both systems were easy to remember but said they preferred DoodlePass. The number of children preferring DoodlePass was 22, compared to 25 who said they thought it was easier to remember. Again, there was the split in preferences between the two systems was not even, with 59.5% of children saying they preferred DoodlePass, 37.8% saying they preferred text password, and one (2.7%) preferring both systems. A chi-square test showed that there was a significant tendency to think that the DoodlePass was preferred compared to a text password (comparing all three options: chi-square = 18.2, df = 2, $p < 0.000$; comparing only text password and DoodlePass: chi-square = 1.78, df = 1, $p = 0.18$). Table 4.24 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 3.74, df = 4, $p= 0.47$; comparing only text password and DoodlePass: chi-square = 1.65, df = 2, $p= 0.44$).

Table 5.24 Breakdown of preference for DoodlePass and text password by children's grade (N = 37)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
DoodlePass	8 66.7%	5 41.7%	9 69.2%	22 59.5%
Text password	4 33.3%	6 50%	4 30.8%	14 37.8%
Equally preferred	0 0.0%	1 8.3%	0 0.0%	1 2.7%

In Session 4, children were asked whether they thought remembering three doodles for DoodlePass or two doodles would be harder (Q1). This was answered by 27 children. 81.5% of children said they thought there would be no difference in memorability for two or three doodles, while 18.5% of children said they thought three doodles would be harder. A chi-square test showed that there was a significant tendency to think that the two and three doodles for DoodlePass are the same in terms of memorability (chi-square = 10.7, df = 1, $p = 0.001$). Table 4.25 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (chi-square = 4.59, df = 2, $p = 0.10$).

Table 5.25 Breakdown of preference for two or three doodles in DoodlePass for ease of remembering by children's grade (N = 27)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
Same	10	8	4	22
	83.3%	100%	57.1%	81.5%
Harder	2	0	3	5
	16.7%	0.0%	42.9%	18.5%

In addition, children were asked whether they thought they will remember their DoodlePass for long time (Q2). Again, this was answered by 27 children. 63% of children said they thought they could remember their DoodlePass for long time, 14.8% of children said they did not think they could, and 22.2% of children were not sure. A chi-square test showed that there was a significant tendency to think one could remember DoodlePass for long time (comparing all three options: chi-square = 10.89, df = 2, p = 0.004; comparing only "Yes" and "No": chi-square = 8.05, df = 1, p = 0.005). Table 4.26 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 2.35, df = 4, p = 0.67; comparing only "Yes" and "No": chi-square = 1.98, df = 2, p = 0.37).

Table 5.26 Breakdown of ease of remembering DoodlePass for long time by children's grade (N = 27)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
Yes	7	5	5	17
	58.3%	62.5%	71.4%	63%
No	3	1	0	4
	25%	12.5%	0.0%	14.8%
Maybe	2	2	2	6
	16.7%	25%	28.6%	22.2%

In Session 5, children were also asked whether they found it easy or hard to remember DoodlePass after 9 months break (Q1). This was answered by 22 children. 68.2% of children said they found it easy to remember DoodlePass, 22.7% of children found it hard, and only 9.1% children said average. A chi-square test showed that there was a significant tendency to be able to remember DoodlePass easily for long time (comparing all three options: chi-square = 12.64, df = 2, p = 0.002; comparing only easy and hard: chi-square = 5, df = 1, p = 0.03).

Table 4.27 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 5.28, df = 4, p = 0.26; comparing only easy and hard: chi-square = 3.7, df = 2, p = 0.16).

Comparing the children's answer for memorability after long period of time according to their answers in Session 4 Q2 and Session 5 Q1, 40% of children who are not sure they could remember DoodlePass after long time of period, find it easy to remember it after 9 months and the same percentage of children find it hard. Interestingly, 71.4% of children who said yes, I can remember DoodlePass after long period of time, found it easy and only 21% found it hard. Moreover, all children who indicated they would not remember DoodlePass after long period of time, actually found it easy to remember after 9 months.

Table 5.27 Breakdown of difficulty level to remember DoodlePass by children's grade (N = 22)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
Easy	5	5	5	15
	55.6%	71.4%	83.3%	68.2%
Hard	4	1	0	5
	44.4%	14.3%	0.0%	22.7%
Average	0	1	1	2
	0.0%	14.3%	16.7%	9.1%

Two questions were asked first in Session 1 and repeated again in Session 5 (Q3. Which do you think easy to remember DoodlePass or text password? and Q4. Which do you prefer DoodlePass or text password?). This was done to measure the perceived and actual memorability and children's preference at the beginning of using DoodlePass (which is new to them in comparison to a text password, and after using it for long period of time. Although the percentage of children thinking a text password is easy to remember increased almost to double in Table 4.28 compared with the result in Table 4.23, and the percentage of children who choose DoodlePass decreased almost half, these changes were mainly in the choices of young children (Grades 1 to 4) while older children (Grades 5 to 6) still gave a higher percentage for DoodlePass in Table 4.28.

54.5% of children thought that a text password would be easy to remember, 36.4% of children thought DoodlePass easier, and only 9.1% of children said both systems are equally easy to remember. A chi-square test showed that there was a significant tendency to think that a text password would be easier to remember (comparing all three options: chi-square = 6.91, df = 2, p = 0.03; comparing only text password and DoodlePass: chi-square = 0.8, df = 1, p = 0.37). Table 4.28 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 2.68, df = 4, p= 0.61; comparing only easy and hard: chi-square = 1.61, df = 2, p= 0.45).

Interestingly, six children who said a text password was easier to remember than DoodlePass said they preferred DoodlePass to a text password. So the number of children preferring DoodlePass was 14, compared to only 8 who said they thought it was easier to remember. Again, there was not an even split in preferences between the two systems, with 63.6% of children saying they preferred DoodlePass, 31.8% saying they preferred a text password, and 4.5% prefer both systems equally. A chi-square test showed that there was a significant tendency to prefer DoodlePass in comparison to a text password (comparing all three options: chi-square = 11.5, df = 2, p = 0.003; comparing only text password and DoodlePass: chi-square = 2.3, df = 1, p = 0.13). Table 4.29 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 6.59, df = 4, p= 0.16; comparing only text password and DoodlePass: chi-square = 4.85, df = 2, p= 0.09).

Table 5.28 Breakdown of preference for DoodlePass and text password for ease of remembering by children's grade (N = 22)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
Text password	6 66.7%	4 57.1%	2 33.3%	12 54.5%
DoodlePass	2 22.2%	3 42.9%	3 50%	8 36.4%
equally easy	1 11.1%	0 0.0%	1 16.7%	2 9.1%

Table 5.29 Breakdown of preference for DoodlePass and text password by children's grade (N = 22)

Child Answer	Grades 1 & 2	Grades 3 & 4	Grades 5 & 6	Total
DoodlePass	5 55.6%	3 42.9%	6 100%	14 63.6%
Text password	3 33.3%	4 57.1%	0 0.0%	7 31.8%
equally preferred	1 11.1%	0 0.0%	0 0.0%	1 4.5%

A summary of the categories of the answers given to explain how children remembered their DoodlePass after long period (9 months) is given in Table 4.30. 19 of the 22 children were able to give an answer to this question (86.4%), 1 child in grade 6 said *"I do not know"* (P2, G6) while two children in Grade 1 did not give an explanation of how they remember DoodlePass (e.g., P13, G1, *"because I know I remember"*). The most commonly mentioned reasons are that the child draw it by themselves (47.4%). One surprise answer from a child in grade 1 was that he redraws his doodles at home to avoid forgetting them, as he explains verbally to me while answering: *"because I see it at home I can remember"* (P9, G1).

Table 5.30 Reasons given for how children remembered their DoodlePass after 9 months (N = 19)

Reasons	Examples	Frequency
Child own drawing	Because it is my draw (P1, G3)	9 47.4%
Draw (things child love, things child used to draw, things in the room that the child registered his Doodles in, things related to school lesson)	because these are the one that I love (P7, G3)	5 26.3%
Child can recognise his draw/ colouring	I know it when I see it (P3, G2)	4 21.1%
Child saved a copy of his doodles at home	because I see it at home I can remember (P9, G1)	1 5.3%
Child use the DoodlePass many times	because it is the same (P26, G1)	1 5.3%
Child have good memory	I have good memory (P17, G3)	1 5.3%

5.4 Discussion

The DoodlePass authentication system was analysed according to different usability aspects: effectiveness, efficiency, and satisfaction. In term of effectiveness, most of the children who are aged 6-12 years successfully recognise and select their doodles at login in all sessions on their first attempt. A few children needed a hint (4th attempt) or for the researcher to tell them the correct DoodlePass (5th attempt), all of whom are younger children in grades 1 to 3. While observing children using the DoodlePass authentication system, it appears that their wrong choices, in the first four sessions, were either related to having difficulties to recognise the correct order for the doodles or clicking on the submit/next button without selecting a doodle. Therefore, in Session 5, all incorrect attempts were recorded, and they were divided to three types: selecting correct doodles but in the wrong order (56.3%), selecting a doodle similar to the child's doodles but not their actual doodle (21.9%), or a wrong doodle neither belonging to the child's selected doodles nor similar to the child's doodles (21.9%). Although the order of doodles was minor problem in this study, it is worth noticing that 5 children mentioned verbally that order was one of the difficulties they encountered, and this is also reported by Mendori et al. (2005) and Cole et al (2017). Overall, in the DoodlePass authentication system 98.5% of children successfully logged in after a short term gap within each session, after a medium term gap between each week, and after a long term gap of nine months. Most children in this study claimed that because their password is their own drawings this helped them to remember their doodles or at least recognise it among other doodles in the grid. Hence, the DoodlePass authentication system is very effective when compared with other systems proposed in the literature. Read and Cassidy (2012) in their results reported that 23.1% of children (aged 6 to 7 years) who created a text password failed to recall it after an hour, Renaud (2009a) reported only 87% of children (aged 11-12 years) could recognise their graphical password when tested twice with a three month gap between the two logins. However, this is in contrast to outcome of Cole et al. (2017) who found that children (aged 6 to 12 years) could recognise their self-generated text password with higher success rates than graphical password.

In term of efficiency, children needed less than 10 seconds on average to recognise and select the doodle in each grid with certain amount of practice. Therefore, overall login using three doodles is typically less than 30 seconds, which seems reasonable. With respect to age group, as expected older children in Grades 4 to 6 were significantly faster on most occasions than

younger children in Grades 1 to 3. In this study there were no control condition of a text password to compare login time, nor was there comparable data from any similar systems (Renaud, 2009a; Stewart et al., 2020) discussed in the literature review chapter (see Table 2.2 in Chapter 2, section 2.3) In addition, I was unsure whether the DoodlePass authentication system would be effective, so I did not want to add more load on children by asking additional tasks such as creating and using a text password. In addition, there were issues of how long each session could be, taking into account time constraints in meeting children during school time.

With regard to satisfaction, most children at the beginning of the study thought DoodlePass is easy to remember than text password, however their thoughts changed by the last session. This could have been because of long break of time (9 months) before they used the DoodlePass authentication system for the last time. This was mentioned by one of the children: *"I use my text password every day, so I remember it, but DoodlePass long time did not use takes time to remember"*. In contrast to that, most children at the beginning and end of the study still preferred DoodlePass more than text passwords, this confirms the results from Stewart et al., 2020 although their children were younger. Noting that, all children are newly introduced to DoodlePass authentication system and the preference questions were followed by further questions asking them to explain the reason for their preference, to ensure that 'satisfising' was unlikely to have occurred.

In this study, there were some limitations which are important mention. Firstly, the study was carried out using a laptop which created some accessibility issues. A few children had difficulties using the laptop touchpad in the first few minutes of the first session, as most of the children were used to using touch screen devices. Secondly, in relation to technical issues, at login, if a child accidentally clicked on the Next/Submit button without selecting a doodle, system counted this as a login attempt, which was not appropriate. Thirdly, as the latter part of this study was conducted during the COVID-19 pandemic, this impacted the number of participants who completed the study and also created some technical issues, see below. In terms of number of participants, 15 children out of 37 withdrew from the study at different points, most of whom withdrew for Session 5, due to the pandemic. This smaller number of participants made it difficult to conduct further analyses to compare differences, particularly

in effectiveness and efficiency between participants who chose their doodle successfully on the first attempt and those who had to make more than one attempt.

Also to the pandemic, Session 5 was conducted online, and a few children struggled with weak internet connections, and some meetings had to be rescheduled a number of times as children did not know how to enter a Zoom meeting and needed an adult to be with them to help them do this. Another technical issue with the online session was that when choosing their DoodlePass, some children pointed to their screen and said loudly *"this is my doodle"* thinking that I can see their screen in the same way as they could see my screen. However overall, the children's experience in the online Session 5 was very good and they were more excited than when I met them physically. This could have been because at school they were tired from lessons whereas during the pandemic they were at home and bored with the situation, so participating in the study was an interesting diversion.

Further research is needed to compare the types of errors made with the DoodlePass authentication system for children in this age group and their effect on children's performance.

5.5 Conclusions

The DoodlePass authentication system was evaluated in this study as an alternative to text password authentication for young children. Even though the last session of this study was conducted during the COVID-19 pandemic which affected the number of participants and changed the method of conducting the sessions from physical meeting with children to online, most of the children aged 6-12 years could recognise and select the doodles they had created themselves and login successfully in all sessions at the first attempt and within a reasonable time. This study shows that graphical authentication systems have promise as a replacement for text password for children. These results encouraged me to do another study using a different graphical authentication system for children, one based on images that the children select rather than doodles they create themselves (Chapter 5) to compare it with the DoodlePass authentication system, in order to understand which is the more suitable graphical authentication system for children.

Chapter 5

Study 3: ObjectPass: An Authentication System Suitable for Children

6.1 Introduction

After the promising results achieved with the DoodlePass authentication system in Study 2, I decided to try to improve on this authentication system by changing the type of graphics used. There were two motivations for these changes. Firstly, the type of graphics used in the DoodlePass authentication system were the child's own drawings. Creating and processing the drawings was time consuming as each child needed to draw three different doodles and I had to categorise each doodle and insert it manually into the system. Secondly, I discovered in Study 2 that not all children like to draw, and this was reported by a number of children while drawing their doodles for the DoodlePass authentication system. Another improvement to the research process was to recruit a larger number of participants for this study in order to obtain more accurate results. In addition, the results of Assal et al. (2018) with regard of usability of using objects as an authentication key encouraged me to evaluate objects but using a more scientific methodology of evaluation and different interface in comparison to her work.

In this chapter, a graphical authentication system called ObjectPass was evaluated with 52 children aged 6 to 13 years from three types of schools in Saudi Arabia: a private international school, a private-funded school and a state-funded school. 21 of the children who participated in this study did had participated in the previous study with the DoodlePass authentication system and this was intentional to allow the comparison between the two systems. This is similar to the research by Assal et al. (2018) as they used objects with children aged 7-12 years, but the age group and methodology for the evaluation of the system in my study were different. The ObjectPass authentication system is a web-based system which uses objects familiar to children (i.e., car, mug etc) as an authentication key. In the most complex version of the system, children need to select images of three objects they have selected in the correct order to be authenticated. The system was evaluated for short-, medium-, and long-term effectiveness,

efficiency and satisfaction and the results were promising. All children remembered their ObjectPass objects in the correct order and the majority of children preferred to use ObjectPass in comparison with a text password.

This study addressed the following research questions:

RQ6: Why do children think they need a password?

RQ7: Is the ObjectPass authentication system usable by children aged 6 to 12 years?

6.2 Method

6.2.1 Design

The study used a mixed design, with one between-participants independent variable and two within-participants independent variables. The between-participants variable was the school grade of the children, which ranged from Grade 1 (6 – 7 years old) to Grade 7 (12 - 13 years old) (see Table 5.1). The first within-participants variable was complexity of the ObjectPass authentication system, which involved images of one, two or three objects (e.g., a simple image of a heart). The object images were chosen by the children at the beginning of the study. The second within-participants variable was the login occasion to recognise and selecting ObjectPass, with the same levels as in Study 2 (see Figure 4.2 in Chapter 4, section 4.2.1), four sessions one week apart and a final session approximately three months later (see Figure 5.1) and (see Chapter 4, section 4.2.1) but with different numbers of occasions of using each ObjectPass, depending on the point in the study.

The ObjectPass authentication system tested the children's ability to correctly recognise and select their own object images displayed in a series of 3 x 3 grids with a range of distractor object images (see Figure 5.2), thus creating a child-appropriate authentication system (see Chapter 4, section 4.2.1).

The four dependent variables were the time taken to choose which objects the child in the ObjectPass system, done on the registration page (candidate objects); the time taken to choose order of the objects in ObjectPass, done on key registration page (key objects), the accuracy of recognising and selecting of the objects images during login (as measured by number of errors

in recognising and selecting an object correctly and number of errors in selecting the correct order of the objects), and the time taken to recognising and selecting the objects.

The study involved five experimental sessions, each approximately one week apart (see Figure 5.1), apart from the final session which was approximately three months later.

Each session introduced a more complex authentication key. In Session 1, children were shown images of 27 objects all from different categories (in a 3 x 9 grid) and they chose the first object. Then they were shown a screen of different objects from all the categories, apart from the one they had just chosen, so 26 objects, and they chose a second object. Finally, they were shown a screen of new objects from all the categories, apart from the two they had already chosen, so 25 objects, and they chose a third object.

Each experimental session consisted of a number of parts (see Figure 5.1), these parts happened in different orders depending on the session, as in Study 2 (see Chapter 4, section 4.2.1).

It was initially planned that the sessions would happen face-to-face, to allow exact comparison with Study 2. However, due to the ongoing COVID-19 pandemic, all sessions were conducted via Zoom.

The design dimensions considered in this authentication system was based on general children cognitive abilities as explained in (Chapter 4, section 4.2.1) with one exception for this system. Objects is used as an authentication key; all objects were selected based on the children's choices for the DoodlePass authentication system and no objects unfamiliar to the children were used, such as different type of buildings.

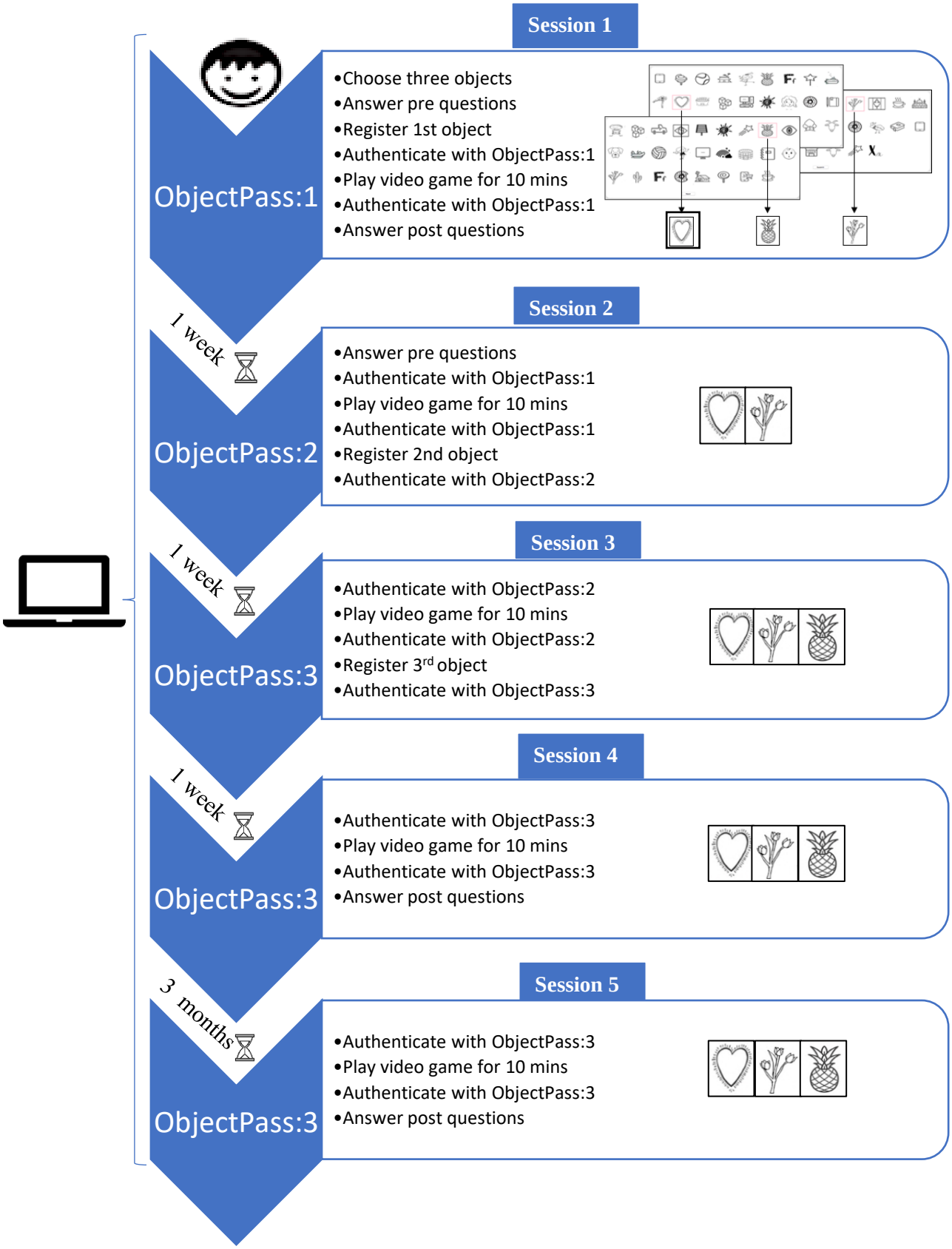


Figure 6.1 Overview of the design of ObjectPass authentication system

6.2.2 Participants

52 children took part in the study, 21 had participated in Study 2 and 31 were new participants. All participants were from a private international school, a private-funded school and a state-funded school in Saudi Arabia (see Table 5.2). The children comprised 26 boys and 26 girls and were aged from 6 to 13 years (see Table 5.1) (see Appendix A.4 for more details regarding the differences between private international, privately-funded, and state-funded schools in Saudi Arabia in terms of English and Computer curricula). The choice of Saudi children is explained in section 4.2.2.

The children used a range of digital devices, the most popular being smartphones, used by 38 (73.1%) of the children, followed by tablet computers (used by 30, 57.7%) and desktop/laptop computers (30, 57.7%) then game consoles (26, 50%). 51 of the children (98.1%) had some experience with passwords and authentication systems, either for accessing digital devices or online accounts. Four of them initially said they had no experience with passwords, but in subsequent questions said they did, so it is assumed that they answered incorrectly to the first question. Only one child did not have an experience with passwords and authentication systems.11 children (21.6%) had used passwords for digital devices only, a further 38 (74.5%) used them for digital devices and online accounts, while no children used them for online accounts only, another two children were unclear in their answers.

Table 6.1 Distribution of all participants for ObjectPass authentication system

Grade	Age (Years)	Gender Distribution	Number of Participants
1	6-7	3 boys, 3 girls	6
2	7-8	5 boys, 4 girls	9
3	8-9	5 boys, 3 girls	8
4	9-10	5 boys, 4 girls	9
5	10-11	3 boys, 3 girls	6
6	11-12	2 boys, 6 girls	8
7	12-13	3 boys, 3 girls	6
Total		26 boys, 26 girls	52

Table 6.2 Distribution of new participants and participants who had participated in DoodlePass and ObjectPass authentication systems

Grade	Gender Distribution for Participants from Study 2	Number of Participants from Study 2	Gender Distribution for New Participants	Number of New Participants
1	-	0	3 boys, 3 girls	6
2	3 boys, 2 girls	5	2 boys, 2 girls	4
3	3 boys, 1 girl	4	2 boys, 2 girls	4
4	4 boys, 2 girls	6	1 boy, 2 girls	3
5	-	0	3 boys, 3 girls	6
6	4 girls	4	2 boys, 2 girls	4
7	2 girls	2	3 boys, 1 girl	4
Total	10 boys, 11 girls	21	16 boys, 15 girls	31

The children were offered a gift voucher worth 50 Riyal (approximately USD 13) to spend at a local bookstore for participating in the study.

6.2.3 Materials and equipment

A website was developed to present the ObjectPass 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 ObjectPass authentication system. The design was very similar to the website used in Study 2, except the initial pages where the children choose their objects.

The website has two versions (Arabic and English). The English version was used with the children who had participated in Study 2, as their level of English was good. The Arabic version was used with the rest of the children, as I was not sure of their level of English. Each child used the same version throughout the study. Figures 5.2 illustrates pages from the website in both English and Arabic.

The website starts with a page on which the researcher enters the child's code, so that the session information is correctly stored. Then the child is transferred either to a login page, a

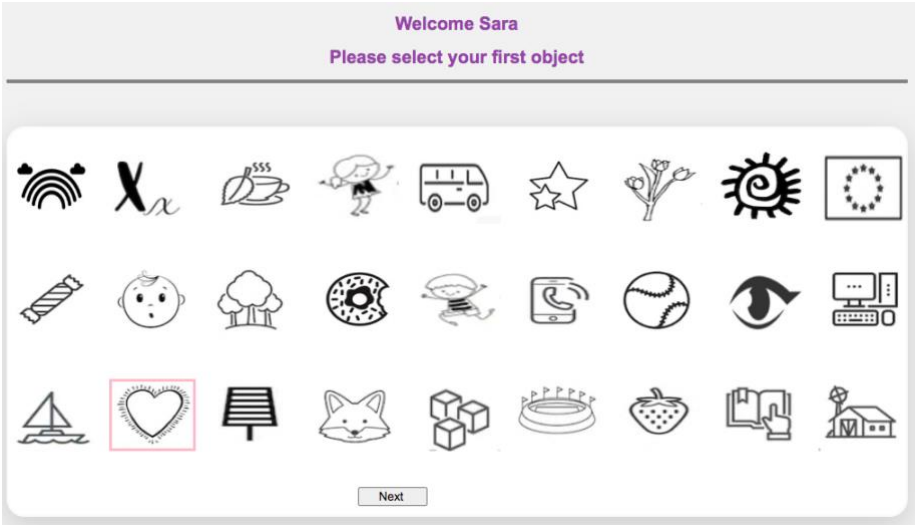
key registration page, or an object registration page. These all have “Welcome” and the child’s name at the top of the page to give the child confidence that the site has recognised them.

On the object registration page, the child chooses images three different objects to form their ObjectPass at different levels of difficulty. This is required only in the first session (see Figure 5.3). The key registration and login pages are the same as in Study 2 (see Chapter 4, section 4.2.3) (see Figure 5.2 and 5.4).

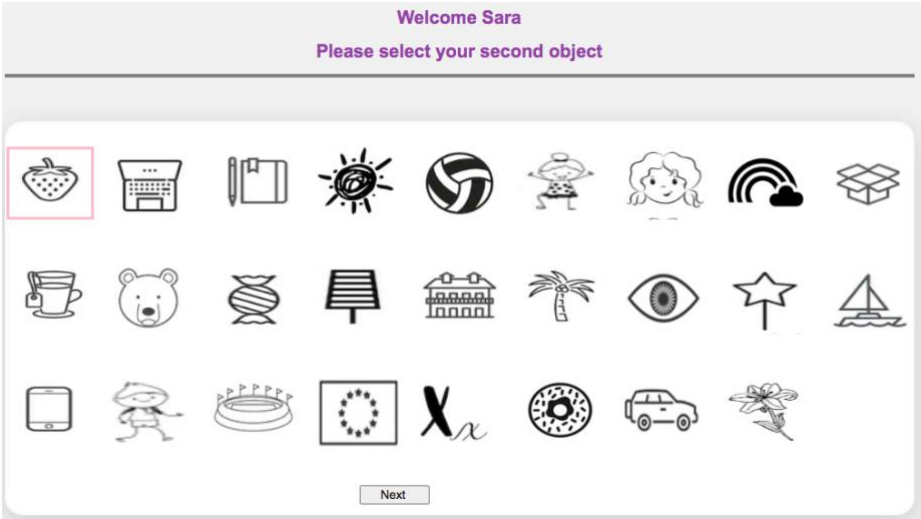
The sequence of accessing the different pages on the website for Session 1 is shown in Figure 5.5, while the rest of the experimental sessions are the same as in Study 2 (see Chapter 4, section 4.2.3).

English version Login page Arabic version Login page

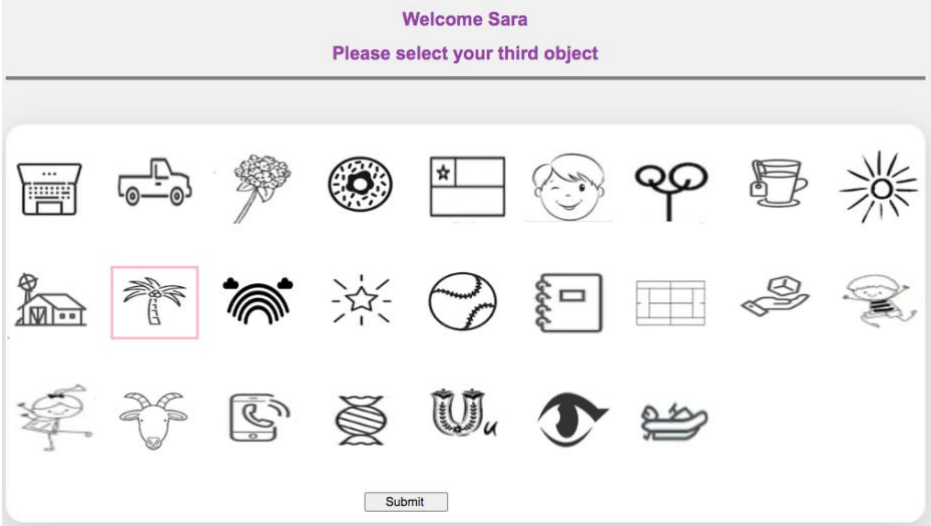
Figure 6.2 Authentication grid of 3 x 3 objects for ObjectPass authentication system (login page)



Registering Object 1



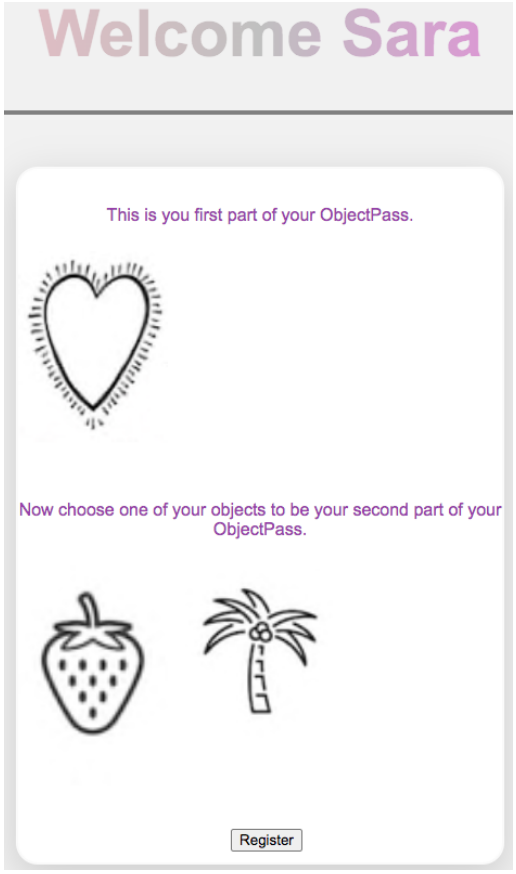
Registering Object 2



Registering Object 3

Figure 6.3 Object Registration pages for ObjectPass authentication system

Creating ObjectPass:1



Creating ObjectPsss:2

Creating ObjectPass:3

Figure 6.4 Key Registration pages in ObjectPass authentication system

The experimental sessions from the researcher's side were all conducted on a 13-inch MacBook Air running MacOS High Sierra (version 10.13.4), with a 1.8 GHz Intel processor. The children used different devices, these are listed in Appendix C.2.

The objects were chosen to be in black and white to avoid children being distracted by colours and at the same time to ensure that children recognise object from the actual drawing and not from the colour. The objects and categories chosen were based on the categories used in Study 2. This meant that the categories would be understood by children in the age range of the study, as examples had been spontaneously drawn by the children in Study 2. It also meant that the categories were at the same level of difficulty as those used in Study 2. There were 27 categories, with 4 objects in each category, making a total of 108 objects which children could choose from for their ObjectPass keys (see Table 5.4).

A selection of games was made from the PBS Kids website (pbskids.org), appropriate for 6 to 13 year old children, these are the same games as used in Study 2 (see Chapter 4, Appendix B.2).

Children who had not participated in Study 2 were asked the series of questions about their password knowledge and use as children had been in Study 2. In Sessions 4 and 5, all children were asked about their experience with ObjectPass authentication system. In Session 5, children who had participated in both studies were asked to compare the DoodlePass and ObjectPass authentication systems (see Table 5.3).

Table 6.3 Open ended questions asked at each experimental session

Session	Questions
1	Questions asked at the beginning of the session for children who participated in ObjectPass authentication system only: 1) Do you have any passwords? 2) Why do you think you need passwords?
2	Questions asked at the end of the session for children who participated in ObjectPass authentication system only: 1) What type of digital devices do you use? 2) Do you use a password to access (each device from previous question)? 3) Do you have any password for online accounts?
3	No questions were asked during this session
4	Questions asked at the beginning of the session for all children: 1) Do you think remembering three objects for ObjectPass much harder than two objects? 2) Do you think you would be able to remember three objects as a ObjectPass for long time?
5	Questions asked at the beginning of the session for children who participated in both Studies 2 and 3: 1) Which one is easier to you to remember DoodlePass or ObjectPass? Why? 2) Which one did you prefer more DoodlePass or ObjectPass? Why? Questions asked at the beginning of the session for all children: 3) Which one is easier to you to remember text password or ObjectPass? Why? 4) Which one did you prefer more text password or ObjectPass? Why?

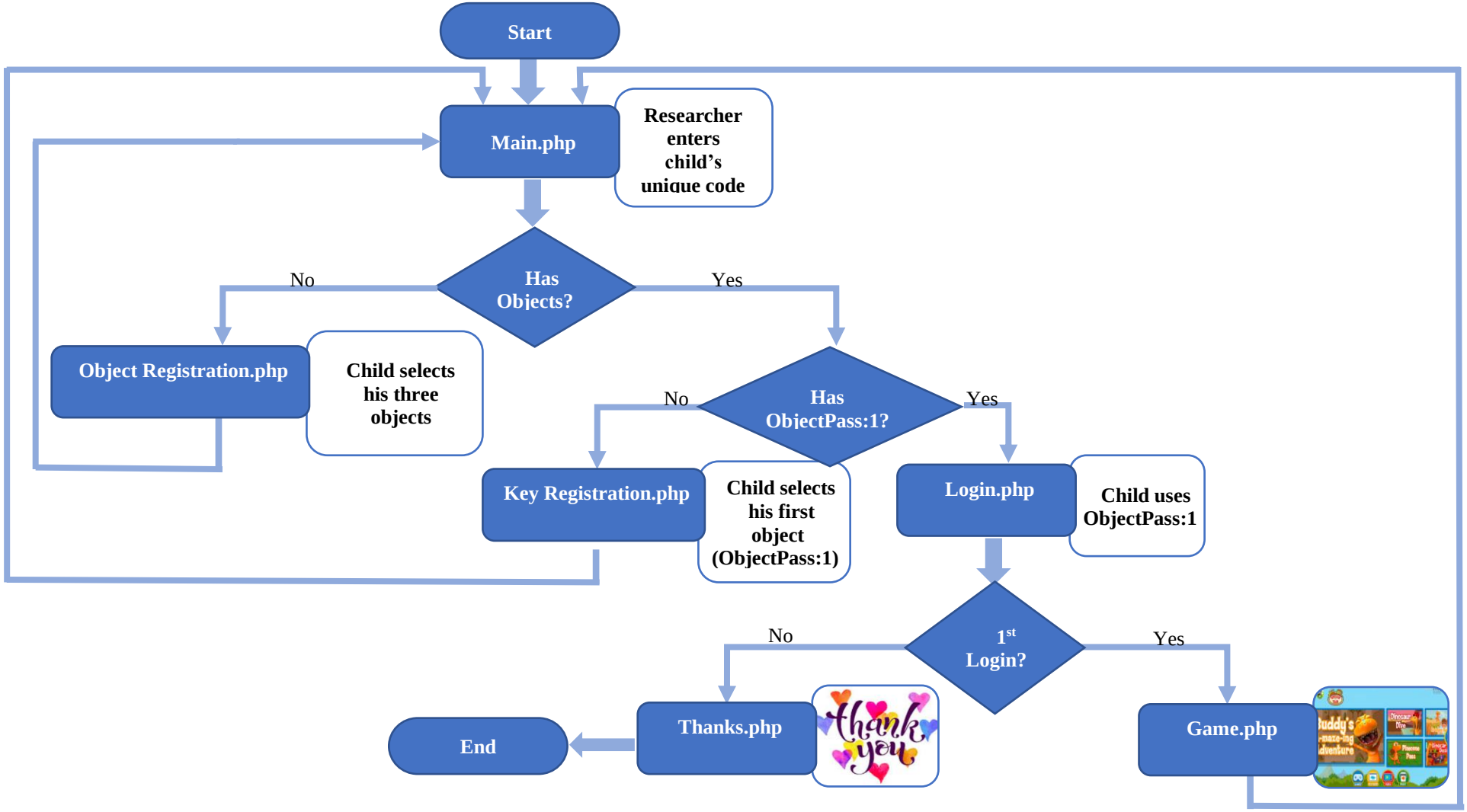


Figure 6.5 Website page sequences for Session1 in the ObjectPass authentication system

6.2.4 Procedure

The study complied with the ethical research principles of the University of York. Following that, a consent letter was sent to parents of children in PDF format (see Appendix C.1). Parents replied to me if they were happy for their child to participate in the study.

As all sessions were online through Zoom, parents were sent several reminders about the sessions to ensure their children attended. Parents received two notification messages via WhatsApp. The first message was sent one day before the meeting date, while the second message was sent 5 minutes before the meeting and contained the Zoom link for the meeting. Although parents knew the importance of their child attending the meeting on the agreed day to ensure the one week (or three months) gap between sessions, parents had the possibility to reschedule meeting time or date if needed. However, it happened very rarely.

At the beginning of Session 1, the children's verbal assent to participate in the research was sought. They were asked if they would help the researcher with their work which would involve creating an online account and logging in to that account a number of times. If they did so they would be able to play video games and receive a gift voucher at the end of the study. They were then asked to choose three objects. They were also told that they had the right to withdraw from the study any time. More details in Chapter 3, section 3.2.4.

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 objects would be used as their password. The rest of procedure for all sessions is the same as for Study 2 (see Chapter 4, section 4.2.4).

During each session, the children answered questions about their use of computing devices, and their knowledge and use of passwords and authentication systems. It was decided to spread these questions out over the different sessions, to avoid overwhelming the children with too many questions at one time (see Table 5.3).

At the end of each session, they were thanked for their participation and told there would be another session in about a week's time, if appropriate. At the end of Session 5 they were thanked for their participation in the study, asked whether they had any questions about the study and given their gift voucher

6.2.5 Data preparation and analysis

Data on a number of the quantitative variables from the study were not normally distributed, so non-parametric statistics were used. It is important to note that (the time to login) in this chapter is calculated based on the first successful attempt for each child (see Chapter 4, section 4.2.5 for more detail).

In some questions the effects of the children's age/grade were investigated. However, this study unlike Studies 1 and 2 in terms of a larger number of participants, so the children were not grouped into levels of two grades (see Chapter 3, section 3.2.1).

To analyse data from the open-ended questions a thematic analysis was used. These were:

Q2 in Session 1. Why do you think you need passwords?

Q3 in Session 5. Which one is easier to you to remember text password or ObjectPass? Why?
Q4 in Session 5. Which one did you prefer more text password or ObjectPass? Why?

The last two questions will be analysed in Chapter 6, in which DoodlePass and ObjectPass are compared:

Q1 in Session 5. Which one is easier to you to remember DoodlePass or ObjectPass? Why?

Q2 in Session 5. Which one did you prefer more DoodlePass or ObjectPass? Why?

The thematic analysis was conducted in a number of steps. First, my supervisor and I met and discussed an initial framework for the codes. Second, I conducted all the coding using these initial codes. Then I send it back to my supervisor who refined it to a final version. Third, we applied new codes to the participants' answers in two different version and then compared and agreed on a final version. With regard to Q 2 in Session 1. (Why do you think you need passwords?), this was asked to all participants in Studies 1, 2, and 3 so all the answers are gathered in this chapter and analysed.

For Q4 Session 5 (Which one did you prefer more text password or ObjectPass? Why?), in some cases the children's answers were analysed according to the actual answer they gave and sometimes according to their answers in Q3 Session 5 as a reason given for thinking ObjectPass

or text password is easier to remember. In addition, the coding for Q4 Session 5 is first derived from the codes for Q3 Session 5 and then further codes were added if needed. This was to link both questions and understand the children answers fully. For example, one child (P30, G7) chose in Q3 Session 5 "*ObjectPass, the reason: Because numbers of pictures is few*". When he answered Q4 Session 5 he said "*ObjectPass, the reason: easier*".

Table 6.4 Categories of objects with examples used in ObjectPass authentication system

Category	Example	Category	Example	Category	Example
Animal		**Ball**		**Boat**	
Book		**Box**		**Boy**	
Candy		**Car**		**Computer**	
Doughnut		**Eye**		**Face**	

Category	Example	Category	Example	Category	Example
Flag		**Flower**		**Football Field**	
Fruit		**Girl**		**Heart**	
House		**Letter**		**Logo**	
Mobile phone		**Mug**		**Rainbow**	
Star		**Sun**		**Tree**	

6.3 Results

Although this study was done during the COVID-19 pandemic through virtual meeting using the Zoom application, no participant withdrew from this study and all participants completed all sessions.

The results in this chapter will be split in to two parts: one that is related to the efficiency of recognising and selecting ObjectPass objects, effectiveness (accuracy) and efficiency (time taken to login) in the ObjectPass authentication system; the other part is related to satisfaction (children's preferences between ObjectPass and text passwords and which do they think is more memorable).

6.3.1 ObjectPass Authentication System

In this section the data that were collected from the children while using the ObjectPass authentication system is analysed separately for each ObjectPass level of difficulty. Thus, when I refer to ObjectPass:1, it means a child's authentication object that is created in the first session and contains their first object. ObjectPass:2, means a child's authentication object that is created in the second session and contains their first and second objects. ObjectPass:3, means a child's authentication object that is created in the third session and contains all three objects. It is important to note that the times in this section are calculated based on first successful attempt for each child.

6.3.1.1 Candidate objects and key objects

This section presents the results of the efficiency, that is time taken to select candidate objects and key objects. For clarification, I refer to the objects chosen at object registration pages (see Figure 5.3) as candidate objects while objects chosen at key registration pages (see Figure 5.4) as key objects.

Candidate objects

Table 5.5 shows the median times for choosing candidate objects with semi interquartile ranges (SIQRs).

Table 6.5 Median times for selecting candidate objects

Candidate Object	Median Chosen Time	SIQR
1	18.5	6.0
2	13.0	4.0
3	13.5	4.0
Total Time	46.0	11.4

To analyse the time to select candidate objects, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed a significant difference between the three objects, FM = 30.31, df = 2, $p < 0.000$. To establish exactly where this difference lay between the different objects, a related samples Wilcoxon test was conducted between the choice times for objects 1 and 2. This showed a significant decrease between the two times (W = - 4.07, $p < 0.000$). A related samples Wilcoxon test was also conducted between the choice times for objects 2 and 3. This showed no significant difference between the two objects (W = 1.72, $p = 0.085$). In addition, a related samples Wilcoxon test was conducted between the choice times for objects 1 and 3. This showed a significant decrease in time between the two objects (W = - 3.65, $p < 0.000$)

To investigate whether there were age differences between the children in the choice times for objects, independent samples Kruskal-Wallis tests between the 1st to 7th grade groups were conducted on the times for each object. The results are summarised in Table 5.6. This shows that the only significant difference was for object 3.

Table 6.6 Kruskal-Wallis tests of grade differences in overall choosing candidate objects times

Candidate Object	Kruskal-Wallis Observed Value	df	p
1	8.90	6	0.18
2	5.58	6	0.47
3	13.21	6	0.04
Total	9.79	6	0.13

To establish exactly where the differences between the grades lay, a series of Mann-Whitney tests was conducted between the times to choose objects for successive grades. The median

time to choose the third object for each grade is shown in Figure 5.6 and the results of the Mann-Whitney tests are shown in Table 5.7. Figure 5.6 shows a very slight trend in times and generally to faster times as the children get older, but there are several fluctuations in the pattern. However, there are significant increase from Grade 3 to Grade 4. On the other hand, there is a significant decrease from Grade 5 to Grade 6 and when we compare Grade 1 with Grade 7, there is no significant difference (U = - 0.667, p = 0.589).

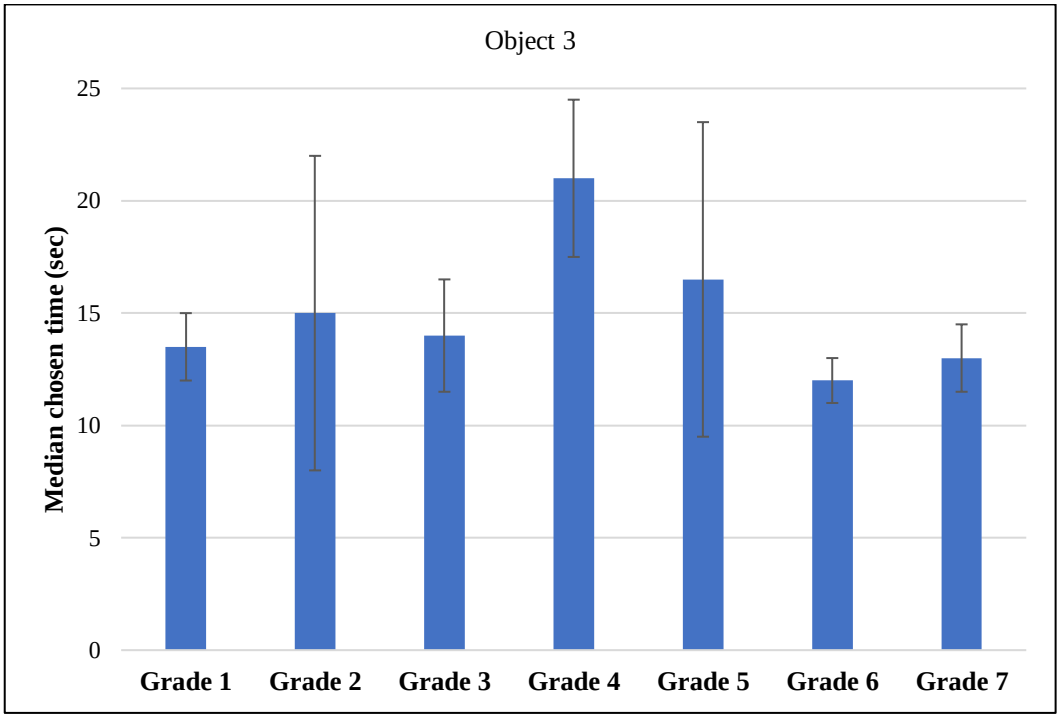


Figure 6.6 Median times for candidate object 3 for children in each grade

Table 6.7 Mann-Whitney tests of differences between grades in time to choose object for candidate object 3 (each grade compared to the previous grade)

Grade	Median Chosen Time	SIQR	Mann-Whitney (U)	p
1	13.5	1.5		
2	15.0	7.0	-0.65	0.53
3	14.0	2.5	-0.97	0.37
4	21.0	3.5	-2.07	0.04
5	16.5	7.0	-0.53	0.61
6	12.0	1.0	-2.12	0.04
7	13.0	1.5	-1.00	0.35

Key objects

Table 5.8 shows the median times for choosing key objects with semi interquartile ranges.

Table 6.8 Median times for selecting Key objects

Key Object	Median Chosen Time	SIQR
1	13.0	2.5
2	12.5	3.0
3	8.0	1.5
Total time	35.0	7

To analyse the time to select key objects, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed a significant difference between the times for the three objects, FM = 41.23, df = 2, $p < 0.000$. To establish exactly where this difference lay between the different objects, a related samples Wilcoxon test was conducted between the choice times for objects 1 and 2. This showed no significant difference between the two times (W = - 0.31, p = 0.96). A related samples Wilcoxon test was also conducted between the choice times for objects 2 and 3. This showed a significant increase between the two objects (W = 5.11, $p < 0.000$. In addition, a related samples Wilcoxon test was conducted between the choice times for objects 1 and 3. This showed a significant decrease in time between the two objects (W = 5.22, $p < 0.000$).

To investigate whether there were age differences between the children in the choice times for objects, independent samples Kruskal-Wallis tests between the 1st to 7th grade groups were conducted on the times for each object. The results are summarised in Table 5.9. This shows no significant difference.

Table 6.9 Kruskal-Wallis tests of grade differences in overall choosing key objects times

Key Object	Kruskal-Wallis Observed Value	df	p
1	3.47	6	0.75
2	5.72	6	0.46
3	8.14	6	0.23
Total	4.31	6	0.64

6.3.1.2 ObjectPass:1

In this section I will now refer to the key objects simply as objects for brevity. Table 5.10 shows the accuracy (recognition and selection of the correct object on the first attempt or subsequent attempts) and median times for successful first attempts (with semi interquartile ranges) for ObjectPass:1, across the four presentations of ObjectPass:1 in Sessions 1 and 2. These median times are also illustrated in Figure 5.7.

Table 6.10 Accuracy and times for login with ObjectPass:1

Session	Login Number	Login Accuracy	Median Login Time (Successful 1st Attempts)	SIQR
1	1	52 on first attempt (100%)	10.0	2.5
	2	52 on first attempt (100%)	9.0	3.5
2	1	50 on first attempt (96.2%) 2 on second attempt (3.8%)	11.0	3.0
	2	52 on first attempt (100%)	9.0	2.5

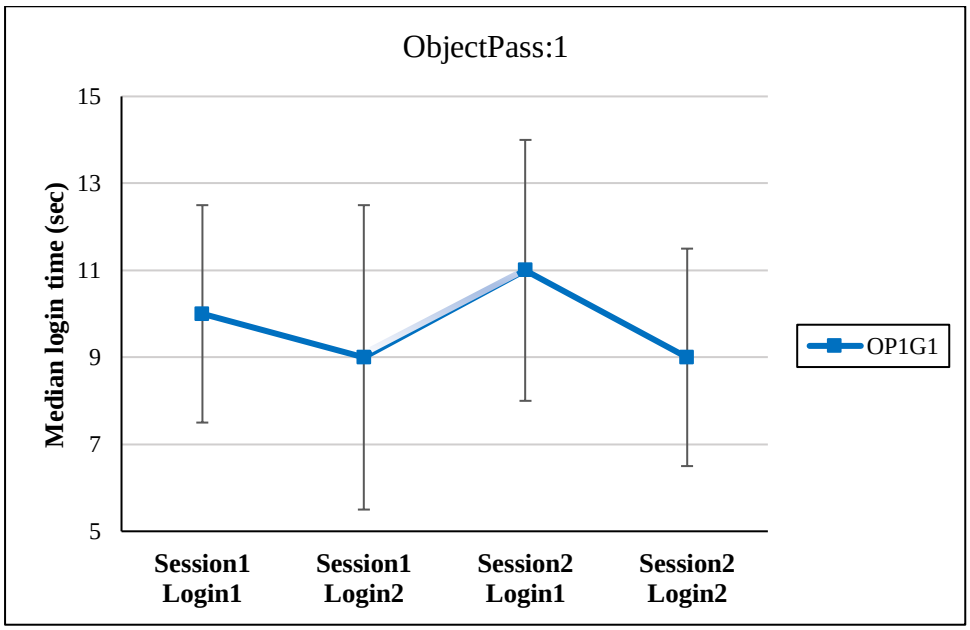


Figure 6.7 Median times and semi interquartile ranges for successful first logins for ObjectPass:1
Note: Shaded line indicates the one week gap between Session 1 and Session 2

The accuracy figures in Table 5.10 show that almost all the children were able to remember their ObjectPass:1 on all occasions. On only two occasions out of a total of 208 (52 children x

4 logins), so 0.96% of occasions was a second attempt needed. Two children needed a second attempt to remember their ObjectPass:1 on the first login in Session 2, so one week after they had created and used the ObjectPass:1. With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the times to select ObjectPass:1 on the different login occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed a significant difference between the four logins, FM = 18.29, df = 3, $p < 0.000$. To establish exactly where this difference lay between the different logins, related samples Wilcoxon tests were conducted between the login times for the two logins in Session 1 and in Session 2. Both of these showed a significant decrease from the first login to the second login in the session (Session 1: W = -2.05, p = 0.04; Session 2: W = -2.26, p = 0.02). A related samples Wilcoxon test was also conducted on the login times for the 2nd login in Session 1 and in 1st login in Session 2. This showed a significant increase between the two logins (W = -2.81, p = 0.01). However, as Table 5.10 and Figure 5.7 shows, the interquartile range for Session 1, Login 2 is the longest of the four logins. This shows that at this login some participants remembered their ObjectPass:1 quickly while others took a considerably longer time, and this might be due to the 10 minutes period (distraction time) between logins in Session 1.

To investigate whether there were age differences between the children in the login times for ObjectPass:1, independent samples Kruskal-Wallis tests were conducted between the 1st to 7th grade groups on the times for each login. The results are summarised in Table 5.11. This shows that the only significant difference was at the first login (Session 1, Login 1). To establish exactly where the differences between the grades lay, a series of Mann-Whitney tests was conducted between the login times for successive grades.

Table 6.11 Kruskal-Wallis tests of grade differences in ObjectPass:1 overall login times

Session	Login	Kruskal-Wallis Observed Value	df	p
1	1	12.94	6	0.04
	2	6.60	6	0.36
2	1	5.13	6	0.53
	2	8.74	6	0.19

Figure 5.8 shows the median login times for Session 1, Login 1 for each grade of participants and Table 5.12 shows the results of the Mann-Whitney tests on successive grades. Figure 5.8 shows that the overall trend is for shorter login times as the children get older, although the decreases are not consistent. This is reinforced by Table 5.12, which shows there are no significant differences between successive grades. However, when Grade 1 is compared with Grade 7, there is a significant decrease in login time (U = - 2.82, p = 0.002).

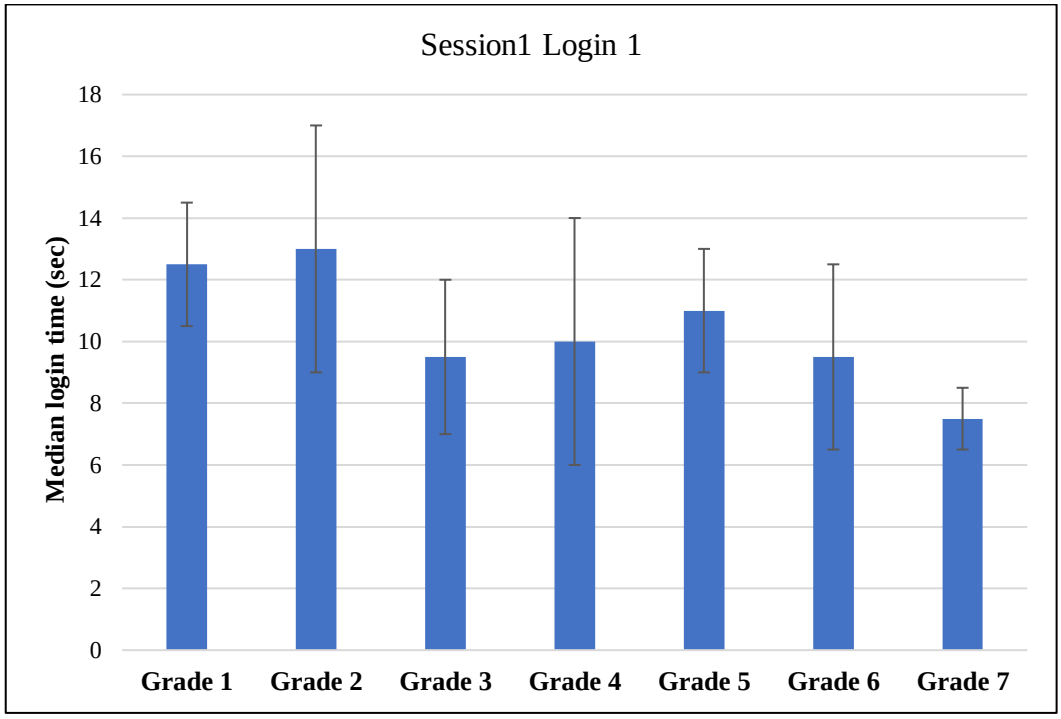


Figure 6.8 Median times for successful first logins for ObjectPass:1 for Session 1, Login 1 for children in each grade

Table 6.12 Mann-Whitney tests of differences between grades in ObjectPass:1 login times for Session 1, Login 1 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	12.5	2.0		
2	13.0	4.0	0.12	1.0
3	9.5	2.5	-1.55	0.14
4	10.0	4.0	0.34	0.74
5	11.0	2.0	-0.77	0.46
6	9.5	3.0	-1.24	-0.23
7	7.5	1.0	-0.92	0.42

6.3.1.3 ObjectPass:2

Table 5.19 shows the accuracy of selecting the correct object (on the first and subsequent attempts) for each of the two grids of objects in ObjectPass:2 and median times for successful first login attempts (with semi interquartile ranges) for each grid. These median times are also illustrated in Figure 5.9.

Table 6.13 Accuracy and times for login with ObjectPass:2

Session	Login Number	Login Accuracy	Median Login Time (Successful 1st Attempts)	SIQR
2	3	Grid1: 52 on 1st attempt (100%)	8.0	2.0
		Grid2: 51 on 1st attempt (98.1%) 1 on 2nd attempt (1.9%)	8.0	2.0
3	1	Grid1: 48 on 1st attempt (92.3%) 4 on 2nd attempt (7.7%)	9.50	2.0
		Grid2: 45 on 1st attempt (86.5%) 5 on 2nd attempt (9.6%) 2 on 3rd attempt (3.8%)	9.0	3.0
	2	Grid1: 51 on 1st attempt (98.1%) 1 on 2nd attempt (1.9%)	9.0	2.5
		Grid2: 51 on 1st attempt (98.1%) 1 on 3rd attempt (1.9%)	6.0	1.5

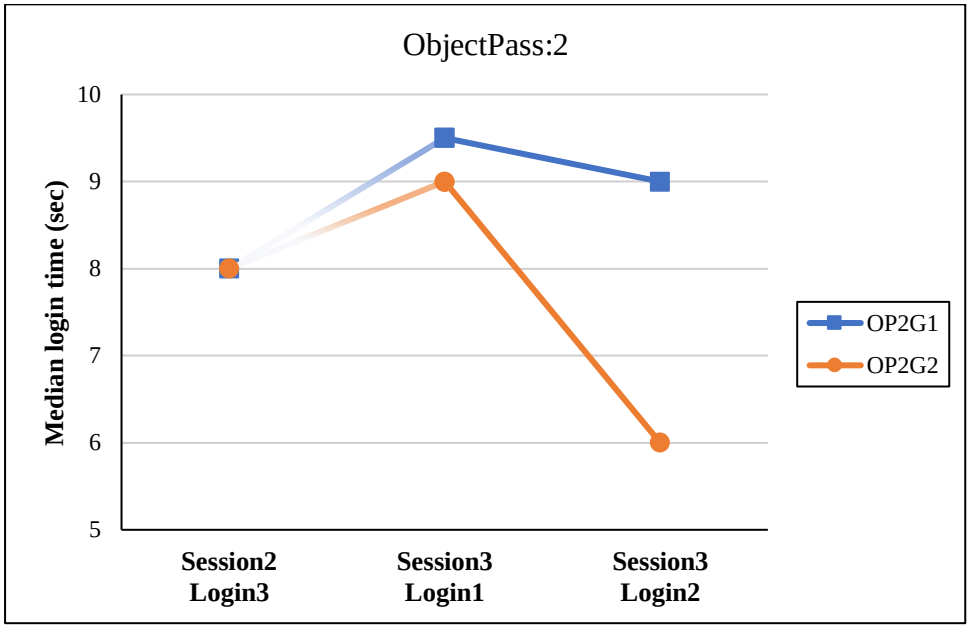


Figure 6.9 Median times for Session 2 and Session 3 logins for ObjectPass:2

Note: OP2G1: ObjectPass:2, Grid 1; OP2G2: ObjectPass:2, Grid 2; Shaded lines indicates the one week gap between Session 2 and Session 3

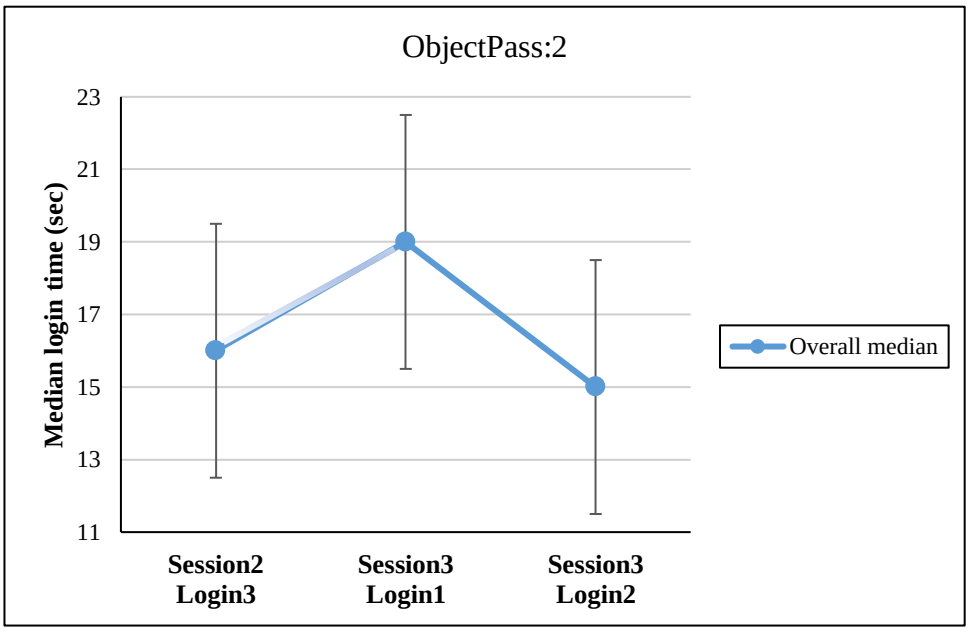


Figure 6.10 Overall median times and semi interquartile ranges for ObjectPass:2

The accuracy figures in Table 5.13 show that children were in general very accurate in selecting the correct objects for ObjectPass:2. On only a small number of occasions did children need a second or third attempt (on 14 occasions out of a total of 312, so on 4.5% of occasions; 11 occasions on the second attempt and 3 occasions on the third attempt). Two children (one child in grade 5: Session 3, Login 1 and 2; one child in grade1: Session 3, Login 2) needed a third attempt to recognise their ObjectPass:2, so one week after they had created and used the ObjectPass:2. With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the differences in the overall login times which were successful at the first attempt on the different login occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed a significant difference between the three logins, FM = 13.54, df = 2, $p < 0.001$. To establish exactly where this difference lay between the different logins, related samples Wilcoxon tests were conducted on the login times for the 3rd logins in Session 2 and in 1st login in Session 3 as well as 1st and 2nd logins in Session3. These showed a significant increase from the third login in Session 2 to the first login in Session 3 (W = 3.45, $p = 0.001$;) and a significant decrease from the first login to the second login in Session 3 (W = -3.56, $p < 0.000$). The semi interquartile ranges, as shown in Figure 5.10, are large for all these logins, suggesting that some children quickly remembered their ObjectPass:2 while others took a much longer time.

To investigate whether there were age differences in the login times for ObjectPass:2, independent samples Kruskal-Wallis tests were conducted on the overall login times which were successful at the first attempt for each login for children in the different grades. The results are summarised in Table 5.14. This shows that there are significant grade differences at Session 2, Login 3 and Session 3, Login 2. To establish exactly where the differences between the grades lay, a series of Mann-Whitney tests was conducted between the login times for successive grades for these two logins.

Table 6.14 Kruskal-Wallis tests of grade differences in overall ObjectPass:2 login times

Session	Login	Kruskal-Wallis Observed Value	df	p
2	3	18.70	6	0.01
3	1	5.96	6	0.43
	2	13.54	6	0.04

For Session 2, Login 3, Figure 6 shows the median overall login times for each grade of children and Table 5.15 show the results of the Mann-Whitney tests on successive grades. Figure 5.11 shows a very slight trend in times and generally to faster times as the children get older, but there are several fluctuations in the pattern. However, there are significant decreases from Grade 1 to Grade 2, from Grade 3 to Grade 4, and from Grade 5 to Grade 6. On the other hand, there is a significant increase from Grade 4 to Grade 5 and when we compare Grade 1 with Grade 7, there is no significant difference (U = -1.60, p = 0.13).

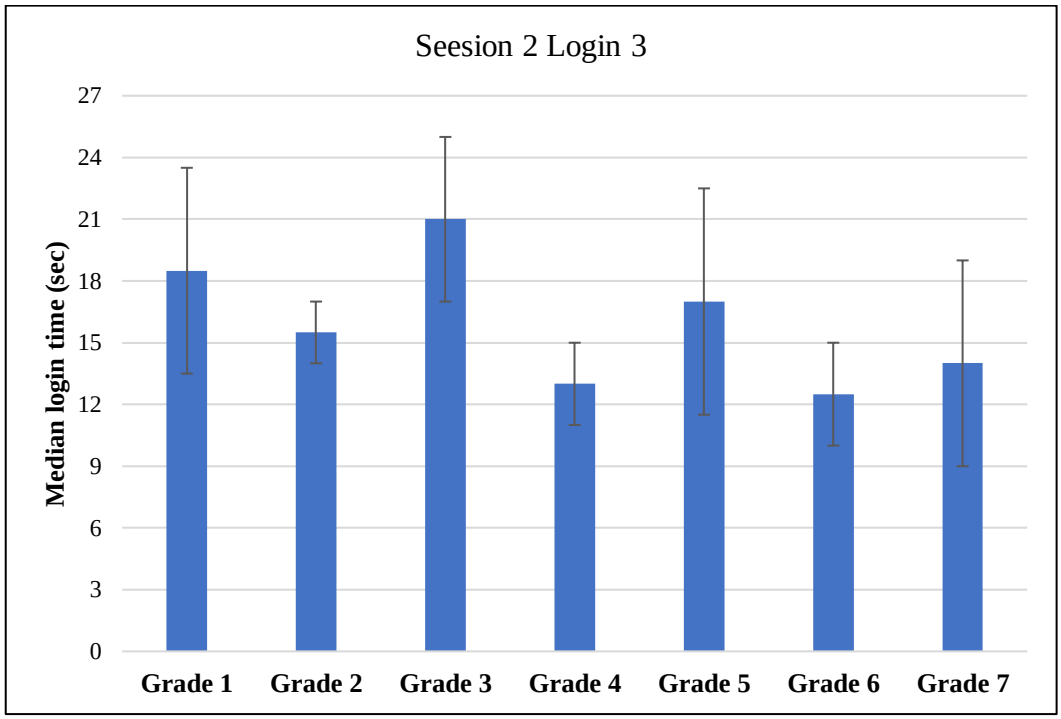


Figure 6.11 Median times for successful first logins for ObjectPass:2 for Session 2, Login 3 for children in each grade

Table 6.15 Mann-Whitney tests of differences between grades in ObjectPass:2 login times for Session 2, Login3 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	18.5	5.0		
2	15.5	1.5	-1.90	0.06
3	21.0	4.0	-1.43	0.16
4	13.0	2.0	-2.71	0.01
5	17.0	5.5	-2.08	0.04
6	12.5	2.5	-2.14	0.03
7	14.0	5.0	-0.91	0.41

For Session 3, Login 2, Figure 5.12 shows the median overall login times for each grade of children and Table 5.16 show the results of the Mann-Whitney tests on successive grades. Figure 5.12 shows that the trend in times is generally to faster times as the children get older, but there are several fluctuations in the pattern. This is reinforced by Table 5.16, which shows there are no significant differences between successive grades. However, when Grade 1 is compared with Grade 7, there is no significant difference (U = -1.65, p = 0.13).

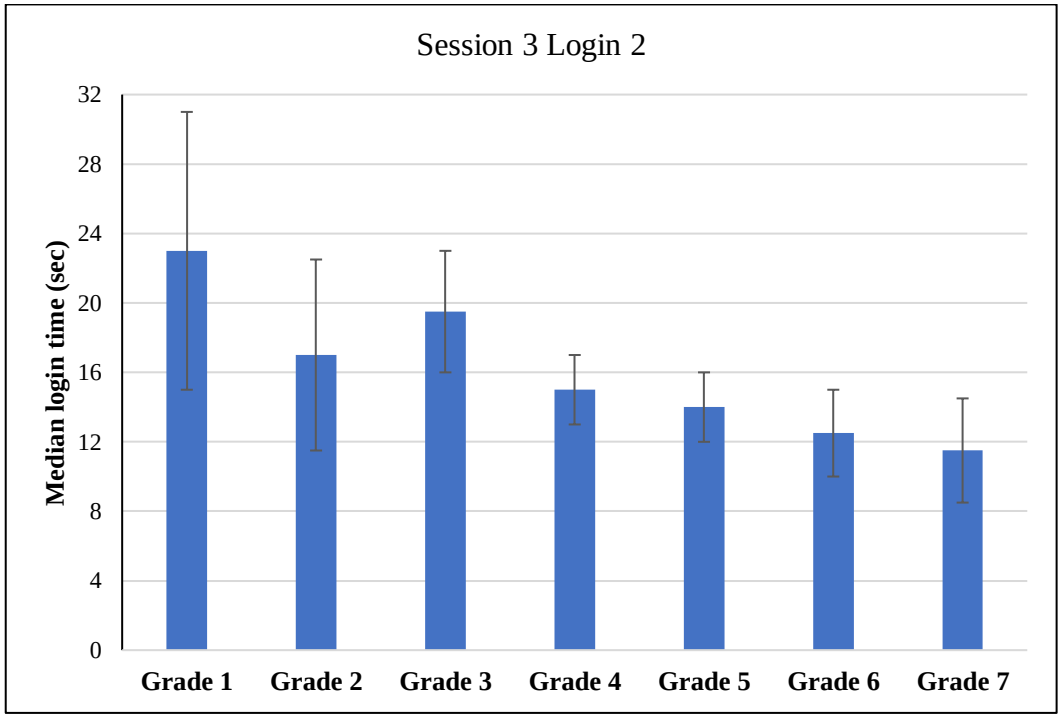


Figure 6.12 Median times for successful first logins for ObjectPass:2 for Session 3, Login 2 for children in each grade

Table 6.16 Mann-Whitney tests of differences between grades in ObjectPass:2 login times for Session 3, Login 2 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	23.0	8.0		
2	17.0	5.5	-0.13	0.90
3	19.5	3.5	-0.15	0.89
4	15.0	2.0	-1.36	0.20
5	14.0	2.0	-0.48	0.70
6	12.5	2.5	-1.26	0.22
7	11.5	3.0	-0.33	0.76

6.3.1.4 ObjectPass:3

Table 5.17 shows the accuracy (selection of the correct object on the first attempt or subsequent attempts) and median times for successful first attempts (with semi interquartile ranges) to select the objects for ObjectPass:3. These median times are also illustrated in Figure 5.13. Figure 5.13shows a jump from Session 3, Login 3 to Session 4, Login 1, this is due to the one week gap There is also another jump from Session 4, Login 2 to Session 5, Login 1, as a result of the approximately three months gap.

Table 6.17 Accuracy and times for login with ObjectPass:3

Session	Login Number	Login Accuracy	Median Login Time (Successful 1st Attempts)	SIQR
3	3	Grid1: 52 on 1st attempt (100%)	7.0	2.5
		Grid2: 52 on 1st attempt (100%)	7.0	2.0
		Grid3: 52 on 1st attempt (100%)	8.0	1.5
4	1	Grid1: 49 on 1st attempt (94.2%) 3 on 2nd attempt (5.8%)	9.0	2.5
		Grid2: 49 on 1st attempt (94.2%) 3 on 2nd attempt (5.8%)	8.0	1.5
		Grid3: 52 on 1st attempt (100%)	9.0	2.0
	2	Grid1: 51 on 1st attempt (98.1%) 1 on 2nd attempt (1.9%)	7.0	1.5
		Grid2: 50 on 1st attempt (96.2%) 2 on 2nd attempt (3.8%)	7.0	1.0
		Grid3: 51 on 1st attempt (98.1%) 1 on 2nd attempt (1.9%)	7.0	2.0
5	1	Grid1: 40 on 1st attempt (76.9%) 12 on 2nd attempt (23.1%)	10.47	3.95
		Grid2: 40 on 1st attempt (76.9%) 11 on 2nd attempt (21.2%) 1 on 3rd attempt (1.9%)	9.98	1.80
		Grid3: 50 on 1st attempt (96.2%) 2 on 2nd attempt (3.8%)	8.22	2.75
	2	Grid1: 49 on 1st attempt (94.2%) 2 on 2nd attempt (3.8%) 1 on 3rd attempt (1.9%)	7.23	1.74
		Grid2: 52 on 1st attempt (100%)	6.67	1.05
		Grid3: 52 on 1st attempt (100%)	6.74	1.21

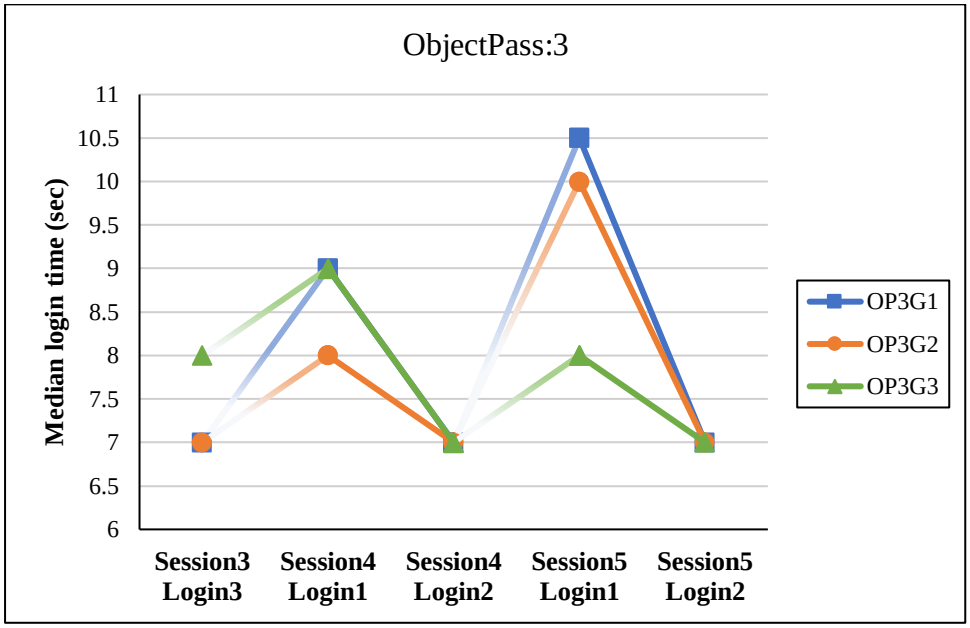


Figure 6.13 Median times for Session 3, Session 4, and Session 5 logins for ObjectPass:3

Notes: (1) OP3G1: ObjectPass:3 Grid 1, OP3G2: ObjectPass:3 Grid 2, OP3G3: ObjectPass:3 Grid 3.
(2) The line between Session 4, Login 1 and Session 4, Login 2 is exactly the same for OP3G1 and OP3G3, but this is not visible.
(3) Shaded line indicates the one week gap between Sessions 3 and 4 and the approx. three month gap between Sessions 4 and 5.

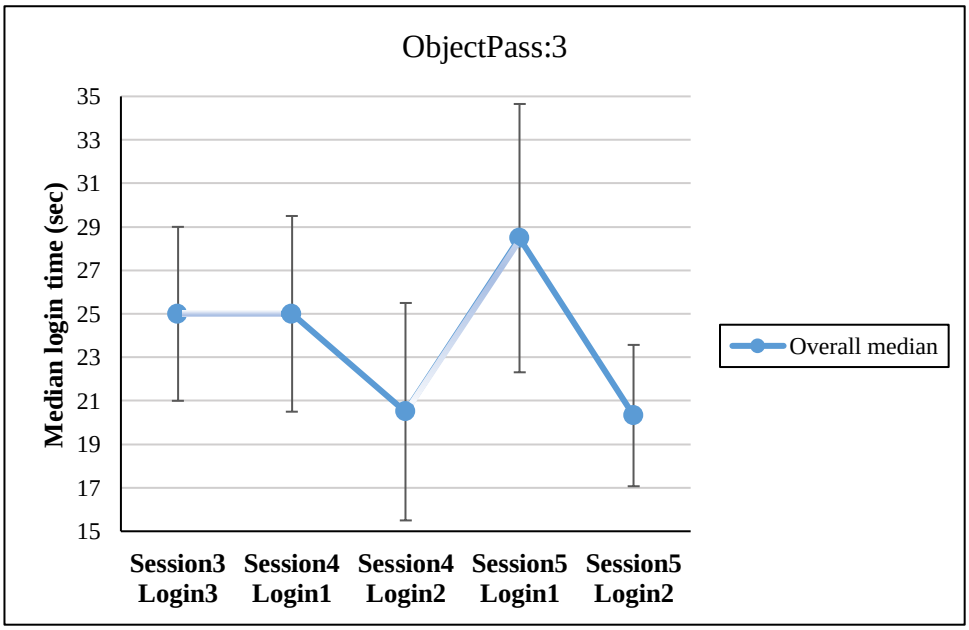


Figure 6.14 Overall median times and semi interquartile ranges for ObjectPass:3

The accuracy figures in Table 5.17 show that almost all the children were able to remember their ObjectPass:3 on all occasions. On only a small number of occasions did children needed a second or third attempt except in first login in Session 5 Grid1 and Grid 2 (39 occasions out of a total of 780, so 5%: 37 occasions on the second attempt and 2 on the third attempt). On both these grids, almost 40% of children needed a second attempt and one child needed a third attempt on Grid 2. However, on Grid 3 only two children needed a second attempt and no children needed a third attempt. So over two months after they had created and used the ObjectPass:3, recognising and selecting rates were still high and it seems that as children got into the recognising task they remembered more. With such high accuracy figures, no inferential statistical analysis was undertaken.

To analyse the overall times to login to ObjectPass:3 on the different occasions, a related samples Friedman's two way analysis of variance by ranks was conducted. This showed a significant difference between the five logins, FM = 33.80, df = 4, $p < 0.000$. To establish exactly where this difference lay between the different logins, related samples Wilcoxon tests were between successive logins both within and between sessions. Table 5.18 shows that there were significant differences in overall times between all successive logins except for Session 3, Login 3 to Session 4, Login 1. However, in the case of the comparison within Session 4 (Login 1 and Login 2) and within Session 5 (Login 1 and Login 2) there were significant decreases, whereas between Session 4 and Session 5 (approximately two months apart) there was a significant increase in overall login time. Going back to Figure 5.14, it is interesting that semi interquartile range for Session 5, Login 1 is greater than the other logins, which suggests that some children in this session could remember their ObjectPass:3 quickly while others took longer time, and this is probably due to the 3 months gap between Sessions 4 and 5.

Table 6.18 Wilcoxon tests of differences in overall login times between successive logins for ObjectPass:3

Login	Related Sample Wilcoxon Test	p
Session 3, Login 3 & Session 4, Login 1	1.68	0.09
Session 4, Login 1 & Session 4, Login 1	-3.77	0.000
Session 4, Login 2 & Session 5, Login 1	3.92	0.000
Session 5, Login 1 & Session 5, Login 2	-3.10	0.002

To investigate whether there were age differences in the login times for ObjectPass:3, independent samples Kruskal-Wallis tests were conducted on the times for each login. The results are summarised in Table 5.19. There was a significant difference only on Session 3, Login 3.

Table 6.19 Kruskal-Wallis tests of grade differences in overall ObjectPass:3 login times

Session	Login	Kruskal-Wallis Observed Value	df	p
3	3	13.58	6	0.04
4	1	6.65	6	0.36
	2	8.29	6	0.22
5	1	10.10	6	0.12
	2	8.19	6	0.22

For Session 3, Login 3, Figure 5.15 shows the median overall login times for each grade of children and Table 16 show the results of the Mann-Whitney tests on successive grades. Figure 5.15 shows that the trend in times is generally to faster times as the children get older, but there are several fluctuations in the pattern. This is reinforced by Table 5.20, which shows there are no significant differences between successive grades. However, when Grade 1 is compared with Grade 7, there is a significant decrease in login time (U = -2.25, p = 0.03).

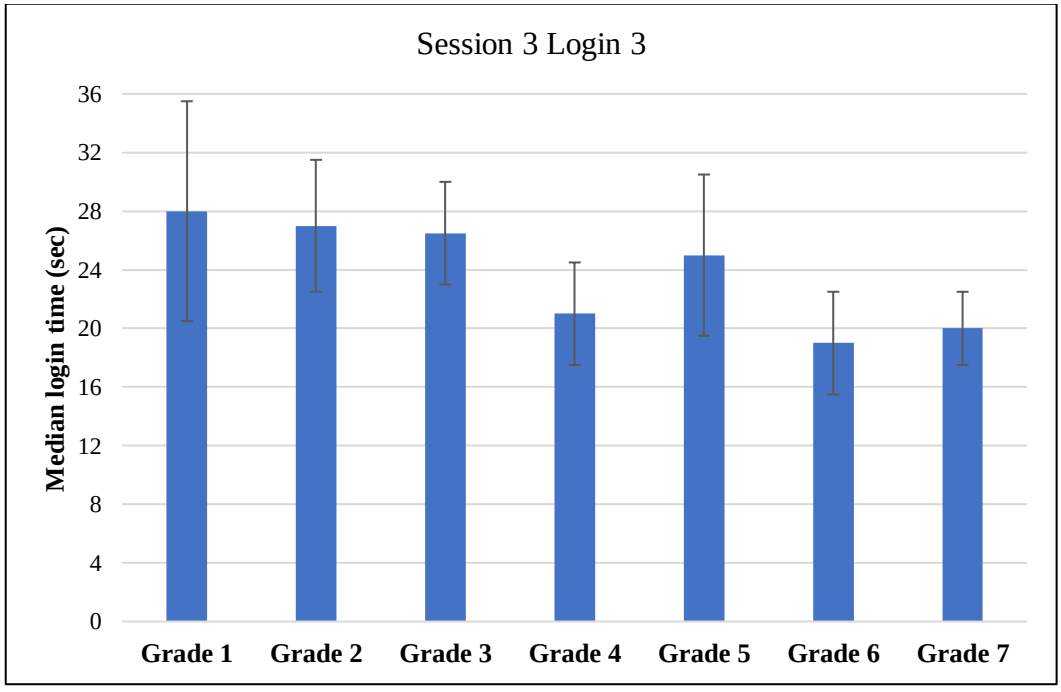


Figure 6.15 Median times for successful first logins for ObjectPass:3 for Session 3, Login 3 for children in each grade

Table 6.20 Mann-Whitney tests of differences between grades in ObjectPass:3 login times for Session 3, Login 3 (each grade compared to the previous grade)

Grade	Median Login Time	SIQR	Mann-Whitney (U)	p
1	28.0	7.5		
2	27.0	4.5	-0.12	0.96
3	26.5	3.5	-0.97	0.37
4	21.0	3.5	-0.58	0.61
5	25.0	5.5	-0.6	0.61
6	19.0	3.5	-1.11	0.28
7	20.0	2.5	0.00	1.00

Table 5.21 shows the number of children who have more than one attempt for each grade of children. This shows that the overall number of attempts decreases with the age of children, although there are fluctuations in percentage between Grades 1 and 2 and Grades 3 to 5. Overall, more than half of attempts (54.5%) were from the younger children (aged 6 - 9 years). This could be due to children's intellectual and cognitive abilities that improve with age. It is interestingly that none of the participants in any age group needed a hint nor for me to tell them which is their ObjectPass in any of the sessions.

Table 6.21 Number of children with more than one attempt while using ObjectPass authentication system for each grade

Number of Attempts	Grade 1	Grade 2	Grade 3	Grade 4	Grade 5	Grade 6	Grade 7
2	8	13	7	7	7	6	2
3	2	0	0	1	2	0	0
Total	10 (18.2%)	13 (23.6%)	7 (12.7%)	8 (14.5%)	9 (16.4%)	6 (10.9%)	2 (3.6%)

6.3.2 Children's preferences between ObjectPass and text passwords

In Session 1, the children were asked "Why do you use passwords?" (Q2) this question was also asked in Studies 1 and 2 as well. A thematic analysis was conducted of their answers. Therefore, answers from all participants in the three studies were combined and analysed in this chapter. 39 children participated in Study 1, 37 children participated in only in Study 2, 31 children participated only in Study 3, and 21 children participated in both Studies 2 and 3, thus

in total there were 107 children, 101 of whom answered this question meaningfully (94.4%). The children who did not answer they said *"I did not know",* and they were all younger children at different grades (3 children in Grade 1, 1 child Grade 2, and 2 children in Grade 3). Table 5.23 summarizes the results of the thematic analysis. The main themes which emerged were:

- **What**: is protected by a password
- **Other's actions**: what actions are others taking that requires the child to have a password
- **Who:** is a password protecting a device/information from
- **Child's actions**: What action is the child taking with a password

Most children's responses contain the type of asset that they want to protect using a password, this information categorised under the "What" theme. Most frequently children mentioned *devices* (61.4%), followed by *things and program* (30.7%). Children also indicate that a password is used to ensure *security, safety and privacy* (19.8%) and this was mostly mentioned by older children (see Table 5.25). A few children mentioned *account* (8.9%) while in the opposite of what was expected, only one child report password used to access his *homework.*

It was also interesting to see "Who" the children thought a password was needed to protect their devices and accounts from. Most frequently mentioned were *non-specific others, others,* and *people in general,* mentioned by 67.3% of children (see Table 5.23) and mentioned by children of all ages. 23.8% of children referred to *the child* owner of the password while only 8.9% of the children referred to *siblings* and *other family members*. Few younger children referred to *other children* and another one younger child referred to *strangers,* this reflects the concrete thinking of the younger children (see Table 5.22). In the other hand, one older child, referred to *hackers.*

In their comments children were also concerned about other children's action which was clear in the responses within theme *other's action* (27.1%). Mostly children want to avoid *unauthorised access* (70.2%) of other children. Children also mentioned *destroy, delete, or damage* action from other (11.9%), followed by *steal* (7.9%). Four older children mentioned *hack or penetrate* and only two children mentioned *search.*

Finally, actions the "Child" was taking by having a password was only mentioned by a small percentage of the children. Reasons for actions included *to prevent access* and *to be secure* (both 9.9%), which were mostly used by older children as shown in Table 5.24, followed by *to have the possibility to access, play, or download* (8.9%) and *to create privacy* (3%). Only one child mentioned *save things*.

It is interesting to note that about a third of the children (31/101, 30.7%) used security words in their answers (e.g., privacy, hack). Most used security words in their responses were from older children (see Table 5.24). However, it may be that younger children here are expressing the same idea, but they are using more concrete ways of describing privacy and security, as they have not learnt these abstract concepts and terms yet.

Table 6.22 Grade breakdown of types of people mentioned in relation to why the child has a password (N= 107)

Grade	**1**	**2**	**3**	**4**	**5**	**6 & 7***
Total number of children answering	**17**	**17**	**16**	**17**	**21**	**19**
Non-specific other	9	11	12	10	13	13
%	52.9	64.7	75	58.8	61.9	68.4
The child	3	3	2	5	7	4
%	17.6	17.6	12.5	29.4	33.3	21.1
Family members	2	1	2	2	1	1
%	11.8	5.9	12.5	11.8	4.8	5.3
Other children	3	1	0	0	0	0
%	17.6	5.9	0.0	0.0	0.0	0.0
Hacker	0	0	0	0	0	1
%	0.0	0.0	0.0	0.0	0.0	5.3
Stranger	0	1	0	0	0	0
%	0.0	5.9	0.0	0.0	0.0	0.0

* In this question only number of children at grade 7 is only 4, so I group it with grade 6

Table 6.23 Reasons given for why you use a password (N = 101)

Theme Frequency (Percentage of Comments)	Sub-Theme Frequency (Percentage of Children Mentioning)	Examples
What is the password protecting? (123, 34.1%)	Device, iPad, computer, mobile (62, 61.4%)	So aunt and their children do not open the device (P88, G1, S3)
	File, program (31, 30.7%)	To download games (P105, G3, S3) To access my school and check my homework (P97, G2, S3)
	Privacy, security, safety (20, 19.8%)	Because no one get into my privacy and watch my iPad (P86, G5, S3)
	Account (9, 8.9%)	So my brother and sister do not enter my account and ruined my stuff (P40, G4, S2)
	Something not specified (1, 1%)	So no one know it (P24, G3, S1)
Who? (107, 29.6%)	People in general (68, 67.3%)	So no one knows our secrets and open my device (P67, G3, S2)
	The child (24, 23.8%)	To access my school and check my homework (P97, G2, S3)
	Family members (i.e., sibling, aunt) (9, 8.9%)	So my brother and sister do not enter my account and ruined my stuff (P40, G4, S2)
	Other children (4, 4%)	So kids do not play with my device (P33, G1, S1)
	Hacker (1, 1%)	To protect my devices from hackers (P90, G6, S3)
	Strangers (i.e., people I specifically do not know) (1, 1%)	Because people who we do not know do not use it (P25, G2, S1)
Other's Action (98, 27.1%)	To gain access (71, 70.2%)	So no one enter without permission, privacy (P50, G5, S2)
	To destroy (12, 11.9%)	So no one ruined and do bad things to my device (P92, G1, S3)
	To steal (8, 7.9%)	No one steal my mobile (P57, G6, S2)
	To hack/penetrate (4, 4%)	So that nobody hacks them (P3, G5, S1) No one can penetrate (P30, G6, S1)
	To be able to search (2, 2%)	So no one can open my iPad or my computer to search (P14, G1, S1)
	To change (1, 1%)	If someone enter they do not change settings (P102, G1, S3)
Child's Action (33, 9.1%)	To prevent access (10, 9.9%)	Prevent others (P53, G5, S2)
	To be secure/to protect (10, 9.9%)	To secure our account (P1, G5, S1) Protect the device (P17, G4, S1)
	Play, access, open, download (9, 8.9%)	To open the mobile (P13, G1, S2)
	To create privacy (3, 3%)	To protect my device if someone steal it (P94, G4, S3)
	Make safe (1,1%)	Safety-make my information safe (P49, G5, S2)

Table 6.24 Security words used in Q2. Why do you use a password? (N=31*)

Security Words	Number of Children	Examples
Private	15 (Grade 1- 6)	So no one enter my device and check my private things (P98, G6, S3)
Protect	9 (Grade 4 -7)	To protect my account (P93, G7, S3)
Security	3 (Grade 2 and 5)	To have security (P89, G5, S3)
Safe	3 (Grade 5 and 6)	To have your things inside the device safe (P91, G5, S3)
Hacker	2 (Grade 5 and 6)	To protect my devices from hackers (P90, G6, S3)
Penetrate	1 (Grade 6)	No one can penetrate (P30, G6, S1)

* two children in this table used two security words.

Table 6.25 Grade breakdown of security words used in Q2. Why do you use a password (N=31)?

Grade	1	2	3	4	5	6 & 7
Total number of children Used security word	1/19	2/16	1/18	6/15	11/19	10/20
%	5.3	12.5	5.6	40	57.9	50

In Session 5, children who participate in this study (52 participants) were asked whether they thought remembering the ObjectPass or a text password is easier (Q3). Overall, 33 (63.5%) children thought the Object Pass would be easier to remember, 14 (26.9%) thought a text password would be easier, and 5 (9.6%) thought they would be equally easy to remember. A chi-square test showed that there was a significant tendency to think that the ObjectPass would be easier to remember (comparing all three options: chi-square = 23.6, df = 2, $p < 0.000$; comparing only text password and ObjectPass: chi-square = 7.68, df = 1, $p < 0.005$). Table 5.26 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 9.28, df = 12, p= 0.68; comparing only text password and ObjectPass: chi-square = 1.79, df = 6, p= 0.94).

Table 6.26 Breakdown of answers to Q3 (Which is easier to remember ObjectPass or text password?) by children's grade (N = 52)

Grade	1	2	3	4	5	6	7	Total
ObjectPass	4	7	5	5	3	6	3	33
Text password	1	2	2	4	1	2	2	14
Equally easy	1	0	1	0	2	0	1	5

A summary of the categories of the answers given to explain their choices is given in Table 5.27. 45 of the 52 children (86.5%) were able to give an answer to this question, one child in Grade 1, 3 children in Grade 2, one child in each of Grades 4, 5 and 7 did not answer the question. The most commonly mentioned reasons for thinking ObjectPass will be easier to remember is that the child could remember pictures, picture's description, or shapes (54.8%). In fact, some children gave negative reasons for using text passwords compared with using ObjectPass in term of memorability (19.4%), children's opinion was that text passwords are not easy to remember or recall. In the other hand, the two most common reasons for thinking text passwords will be easier to remember were the child thinks they can remember or recall their passwords, or that passwords are used more often (42.9%). Interestingly, only two children have a negative issue related to ObjectPass; one of them indicated ObjectPass is not used often, while the other comment was the change of place of objects in the grid every time the child logs in.

More than half of the children (29, 64.4%) only mentioned why they thought their choice was easier to remember, 13 children (28.9%) made an explicit contrast between the two systems (e.g. P29, G7, who preferred text password said *"Because I memorise it long time ago and I use it always but if I use pictures a lot it will be easy"*), and three children (6.7%) only mentioned why they did not prefer the other choice (e.g. P21, G3, who preferred ObjectPass said *"Because numbers is difficult to remember"*).

Table 6.27 Reasons given for thinking ObjectPass or a text password is easier to remember (N = 45)

Reason	Examples	Frequency
Prefer ObjectPass because …		**N = 31**
1) Positive points to ObjectPass		
Child will remember {picture, picture description, shapes}	Pictures I can remember it when I see it (P31, G5)	17 54.8%
General positive statement: good, better, easier	More easier (P19, G7)	6 19.4%
Number of objects are small	Because number of pictures is few (P30, G7)	6 19.4%
Child can recognise objects	quickly you recognise it (P41, G6)	3 9.7%
Give the child options	Because I have options (P1, G4)	3 9.7%
The objects are things the child likes	I like pictures (P22, G1)	1 3.2%
The objects are things related to the child	Because you can choose pictures about you (P41, G6)	1 3.2%
Use of (child appropriate) pictures	Because it has pictures (P13, G2)	1 3.2%
2) Negative points to text password		
Difficult to remember/ recall numbers	Because I do not like to memorise numbers (P7, G4)	6 19.4%
Numbers are easy to forget	Because I might forget numbers (P49, G1)	2 6.5%
Password has large number of elements	Because password is made up of many numbers and letters (P32, G4)	2 6.5%
Child do not like using numbers	Because I do not like to choose numbers It is not good (P16, G1)	1 3.2%
Prefer text password because ….		**N = 14**
1) Positive points to text password		
Child have the ability to remember / recall	Because I remember it each time I use it (P3, G3)	6 42.9%
Password used often	Because I use password always (P6, G4)	6 42.9%
Child likes numbers	Because I like math so I like numbers (P25, G2)	2 14.3%
Password is faster	Because quickly I can do it (P37, G1)	2 14.3%
Elements always in the same order	because the numbers are organised in the same order (P11, G6)	1 7.1%
Child chose a simple password	because I chose 9999 (P44, G5)	1 7.1%
Used in all devices	Because I use password in all of my devices (P34, G5)	1 7.1%
2) Negative points to ObjectPass		
Not used often	ObjectPass I do not use it always (P8, G4)	1 7.1%
Pictures changed places (between trials)	objects places changed over time (P11, G6)	1 7.1%

In Session 5, children were asked whether they would prefer to use ObjectPass or a text password. Overall, 32 (61.5%) children said they would prefer the Object Pass, 16 (30.8%) said they would prefer a text password, and 4 (7.7%) preferred both equally. A chi-square test showed that there was a significant tendency to prefer ObjectPass in comparison to text passwords (comparing all three options: chi-square = 22.77, df = 2, $p < 0.000$; comparing only text password and ObjectPass: chi-square = 5.3, df = 1, p = 0.021).

Table 5.28 shows the breakdown of answers by children's grade, but this does not show any clear trend, confirmed by a chi-square test (comparing all three options: chi-square = 10.61, df = 12, p= 0.56; comparing only text password and ObjectPass: chi-square = 7.,44 df = 6, p= 0.28).

Table 6.28 Breakdown of answers to Q4 (Which is more preferred ObjectPass or text password?) by children's grade (N = 52)

Grade	1	2	3	4	5	6	7	Total
ObjectPass	4	6	6	5	4	6	1	32
Text password	2	2	1	4	1	2	4	16
Equally preferred	0	1	1	0	1	0	1	4

A summary of the categories of the answers given to explain their choices is given in Table 5.29. 48 of the 52 children were able to give an answer to this question (92.3%), one child in Grade 1, one child in Grade 2, and two in Grade 3 did not answer the question. Coding of the answers started with the categories from the ease of remembering question (see Table 5.27) and further categories were added as needed. Four more categories were needed to describe the preferences for ObjectPass and three categories for text passwords. In each case, ease of remembering was added as a category, possibly prompted by the earlier question. Only four categories from the remembering question were not used, that of preferring ObjectPass because the objects are things related to the child, things the child likes, difficult to remember number, and numbers are easily forgotten.

The most commonly mentioned reasons for preferring ObjectPass were use of pictures, a general statement that it was good, and that the child can remember the object (e.g., the picture, its shape). The most commonly mentioned reasons for preferring text passwords were for security and safety reasons.

Most of the children (34, 70.8%) only mentioned why they thought their choice was more preferred, 12 children (25%) made an explicit contrast between the two systems (e.g., P10, G6, who preferred ObjectPass said *"because password has numbers while ObjectPass has pictures more easy"*), and 2 children (4.2%) only mentioned why they did not prefer the other choice (e.g., P16, G1, who preferred ObjectPass said *"Because I do not want numbers it is confusing me").*

Table 6.29 Reasons given for preferring ObjectPass or text password (N = 48) (* = new category from Table 5.26)

Reason	Examples	Frequency
Prefer ObjectPass because …		**N = 32**
1) Positive points to ObjectPass		
Use of (child appropriate) pictures	Because it is good I like the picture idea (P45, G2)	14 43.8%
General positive statement: good, faster, easier	Easy to use (P50, G3)	9 28.1%
Child will remember {picture, picture description, shapes}	Because I can remember it direct (P51, G6)	8 25%
Secure/ novel *	More secure (P11, G6) Because it is new, first time I know that it is good (P43, G6)	3 9.4%
Give the child options	Has a lot of images (P20, G4)	3 9.4%
Number of objects are small	Because it is few (P22, G1)	1 3.1%
Child choose one object at a time*	Because password I need to change it and I need to move my finger but ObjectPass I choose it (P40, G3)	1 3.1%
Child can recognise objects	Because I can identify it quickly (P31, G5)	1 3.1%
2) Negative points to text password		
Child do not like using numbers	Because I do not want numbers it is confusing me (P16, G1)	4 12.5%
Child do not like using password in general*	Because password is boring (P20, G4)	3 9.4%
Password has large number of elements	Because password is much longer (P42, G2)	2 6.3%
Not secure*	Object more secure while numbers others can figure it out quickly (P11, G6)	1 3.1%
Difficult to remember/ recall numbers	Numbers is difficult I need more time to remember it (P31, G5)	1 3.1%
Prefer text password because ….		**N = 16**
1) Positive points to text password		
Secure / safe*	Because numbers are more safe protect from hackers (P1, G4)	6 37.5%
Password used often	Because I used to (P2, G7)	4 25%
Child likes numbers	Because I like numbers (P5, G4)	4 25%

General positive statement: faster, easier	Because it is easy to use (P14, G6)	4 25%
Child have the ability to remember / recall	It and it has numbers which is easy to memorise (P2, G7)	2 12.5%
2) Negative points to ObjectPass		
Not used often	ObjectPass I do not use it always (P8, G4)	1 6.3%
Number of objects are small*	I want to have pictures a lot more than 3 then the hacker cannot enter quickly (P34, G5)	1 6.3%
Objects are confusing*	The one that has pictures confuse me sometimes (P18, G7)	1 6.3%

6.4 Discussion

This study aimed to create a graphical authentication system called ObjectPass, that uses objects as the authentication key. The target group for this system was children aged 6-13 years (Grades 1-7). To evaluate the system usability, effectiveness, efficiency, and satisfaction were measured. In term of effectiveness, most children successfully recognised their ObjectPass at login in all sessions on the first attempt and no child needed a hint or help to identify their ObjectPass. As a result of the previous study (Study 2, the DoodlePass authentication system) I realised the importance of recording all type of wrong attempts, hence, in evaluating the ObjectPass authentication system, the wrong attempts were recorded. Less than 5% of all logins involved an error (60/1305, 4.6%). These wrong attempts were either difficulty in recognising and selecting the ObjectPass in the correct order (44/60, 73.3%), or selecting an object similar to the child's objects but not their actual object (16/60, 26.7%). Mendori et al (2005), Read and Cassidy (2012) and Cole et al (2017) all reported that order of authentication key was one of the challenges that children encountered, however, in the ObjectPass authentication system this was only a minor problem. Overall, all children successfully recognised their ObjectPass after a short term period (i.e., within each session), after medium term period (i.e., between each week), and even after long term period (i.e., three months). It is interesting that most children (54.8%) in this study claimed that the reason for recognising their ObjectPass is that it is in the form of image and not alphanumeric characters. In general, the ObjectPass authentication system is very effective when compared with other systems researched in the literature. Assal et al (2018) report that 52% of children (7-12 years old) recognised their graphical password (object) immediately and 88% after 15 minutes. Ratakonda et al (2022) reported that children aged 6-11 years recognised their graphical password after 15 minutes and one week with high success rates compared to text passwords,

and the failed attempts were due to confusing their picture with another picture similar to their password.

In term of efficiency, children needed less than one minute during the registration phase to select three objects and almost half minute to decide the order of these objects to use within their ObjectPass. In relation to time taken to recognise and select their ObjectPass, children needed less than 11 seconds on average for each grid with some practice. Therefore, login using three objects would be less than 33 seconds, which seems reasonable. However, this is in contrast to results found by Ratakonda et al (2022), as they found children took significantly longer time to register and recognise their graphical password compared with text passwords. For age group comparison, as expected older children in Grades 4 to 7 were significantly faster than younger children in Grades 1 to 3 on most occasions. Assal et al. (2018) noted the registration time and login time only as a range of value for all the PassTiles schemes (object, image, and word), they did not give a mean time and standard deviation (or median and semi-interquartile range). This make it difficult to compare the efficiency of those schemes with ObjectPass. This is in addition to the other issues discussed in the literature review chapter (see Table 2.2 in Chapter 2, section 2.3).

With regard to satisfaction, most children thought ObjectPass is easy to remember and preferred it compared to text passwords, the same result was drawn by Assal et al. (2018) when comparing preferences between the three PassTiles schemes object, image, and word). This is largely due to the use of images in the ObjectPass authentication system which most of the children mentioned when giving their reasons in their answers.

With regard to the security aspect of an authentication system, this was not considered when designing ObjectPass authentication system, as the main aim was to ensure usability in the first stage of development and evaluation. Firstly, allowing children to choose their own objects for the authentication key would raise the vulnerability to guessing attacks because children tend to choose objects that contain images of popular toys or their favourite things (Assal et al. 2018). Secondly, using objects means the authentication key is not hashed, so target and distractor objects are not securely stored and vulnerable to dictionary attacks (Stewart et al., 2020). Thirdly, in general this type of authentication key is vulnerable to shoulder surfing attacks (Stewart et al., 2020) especially when the user clicked an object which highlights it (Assal et al., 2018). However, the ObjectPass authentication system minimised the risk of shoulder surfing attack by frequently changing the objects and their position in each grid.

There were a number of limitations to this study. Firstly, participants in the study who had already used DoodlePass authentication system might have been more experienced with the kind of system than other participants, due to the similarities between Doodle and Object pass authentication systems. This could have improved their performance. Secondly, due to the COVID-19 pandemic, the study was all conducted online, and the results may not be as accurate as those from the DoodlePass authentication system study. Finally, there were technical issues which are discussed previously in relation to Study 2 (see Chapter 4, section 4.4).

Thus, I would recommend that future work compare usability issues (effectiveness, efficiency, and satisfaction) and the types of incorrect choices between children who have used more than one kind of graphical authentication system and those who have not. For example, those who have already used the DoodlePass authentication system and those who then use ObjectPass authentication system, to see if this affects the result. Another solution would be to counterbalance the order in which participants experience different kinds or versions of graphical authentication systems. This was not possible in the current studies, as the ObjectPass authentication system was developed and evaluated only after the DoodlePass authentication system had been evaluated, and its development depended on the lessons learnt in the evaluation of DoodlePass.

6.5 Conclusions

The ObjectPass authentication system was evaluated in this study as an alternative to text password authentication and to the DoodlePass graphical authentication system. Even though all sessions of this study were conducted during the COVID-19 pandemic which required that I meet the children online, all 52 children who participated in this study completed all sessions and none withdrew. In term of results, all children recognised their ObjectPass and logged in successfully within reasonable time in all sessions. From this study it seems graphical authentication system to be a promising replacement for text passwords for children. In the next chapter I will explore the differences between the DoodlePass and ObjectPass authentication systems in relation to the three usability aspects to investigate whether one type of graphical authentication is better in terms of usability than the other, and also whether children prefer one type in comparison to the other.

Chapter 6

Study 4: Comparison of the DoodlePass and ObjectPass Authentication Systems

7.1 Introduction

After the promising results from Study 2 (Chapter 4: DoodlePass authentication system) and Study 3 (Chapter 5: ObjectPass authentication system), a further set of analyses was conducted to compare both systems in term of three usability aspects: effectiveness, efficiency, and satisfaction. 21 children had participated in both Studies 2 and 3, meaning they had used both systems. All participants were from Saudi Arabia and studying at privately funded schools. I compared the results of children starting from DoodlePass:1 in comparison with ObjectPass:1 (in which children used only one doodle or image to authenticate themselves). Then I compared DoodlePass:2 with ObjectPass:2 (in which children used two doodles or images in a set order to authenticate themselves). Finally, I compared DoodlePass:3 with ObjectPass:3 (in which children used all three doodles or images in a set order to authenticate themselves). The results show that the ObjectPass authentication system is significantly more effective, efficient, and satisfying than the DoodlePass authentication system.

This set of analyses addressed the following research questions:

RQ8: Which system was more usable, the DoodlePass authentication system or the ObjectPass authentication system?

RQ9: Does the children's age affect their performance and attitudes towards the DoodlePass authentication system and the ObjectPass authentication system?

7.2 Method

7.2.1 Participants

Data from 21 children who took part in both Studies 2 and 3 were analysed, they had used both the DoodlePass and ObjectPass authentication systems. All participants were from privately funded school at Saudi Arabia. The children comprised 10 boys and 11 girls and were aged from 6 to 12 years (see Table 6.1).

The children used a range of digital devices, the most popular being smartphones, used by (14, 66.7%) of the children, followed by tablet computers (used by 13, 61.9%) and game consoles (9, 42.9%) then desktop/laptop computers (7, 33.3%). All children had some experience with passwords and authentication systems, either for accessing digital devices or online accounts. One child initially said they had no experience with passwords, but in subsequent questions said they did, so it is assumed that they answered incorrectly to the first question. 8 children (38.1%) had used passwords for digital devices only, a further (12, 57.1%) used them for digital devices and online accounts, while no children used them for online accounts only, another one child was unclear in his answers.

Table 7.1 Distribution of participants who had participated in both systems

Grade	Age (Years)	Gender Distribution	Number of Participants
1	6-7	3 boys, 2 girls	5
2	7-8	3 boys, 1 girl	4
3	8-9	4 boys, 2 girls	6
4	9-10	-	0
5	10-11	4 girls	4
6	11-12	2 girls	2
Total		10 boys, 11 girls	21

7.2.2 Data preparation and analysis

To compare data with quantitative variables, two-way repeated measures ANOVA, three-way mixed measures ANOVA, and post hoc comparisons (Bonferroni correction) statistics were used. Although non-parametric statistics were used in the analysis of Studies 2 and 3 (Chapter 4 and 5, respectively), in this analysis I chose to use parametric statistics, in particular analysis of variance (ANOVA). This was because in this analysis I wanted to compare results between Studies 2 and 3, the use of DoodlePass and ObjectPass, but also to take into account the differences due to the sessions and login occasions, as well as differences between children's ages and their preference for either DoodlePass or ObjectPass. Conducting such an analysis with non-parametric statistics would be impossible. Therefore, I used ANOVA, using the Greenhouse-Geisser adjustment of degrees of freedom to account for issues of non-homogeneity of variance. In addition, key significant results were checked with non-parametric statistics and only included if they were also significant with both parametric and non-parametric statistics. In some questions the effects of the children's age/grade were investigated. However, the number of children was small, so the children were grouped into levels of three grades (1 to 3 grade, and 4 to 6 grade). (see Chapter 3, section 3.2.1 for more detail).

To analyse data on the open-ended questions relating to both systems and collected in Study 3 (Chapter 5) a thematic analysis was used. The questions were: Q1 in Session5. Which one is easier to you to remember DoodlePass or ObjectPass? Why? Q2 in Session5. Which one did you prefer more DoodlePass or ObjectPass? Why?

The thematic analysis was conducted in a number of steps. First, my supervisor and I met and discussed an initial framework for the codes. Second, I conducted all the coding using these initial codes. Then I send it back to my supervisor who refine it to the final version. Third, we applied new codes to the participants' answers in two different version and then compare and agree on a final version.

For Q2 Session 5, in some cases the children's answers were analysed according to the actual answer they gave as a reason given for thinking DoodlePass or ObjectPass is easier to remember and sometimes according to their answers in Q1 Session 5. In addition, the coding for Q2 Session 5 is first derived from Q1 Session 5 and then further codes were added if needed.

This was to link both questions and fully understand the children answers. For example, one child (P17, G4) chose in Q1 Session 5 "ObjectPass, the reason: *better because I choose things that is more related to me like the first letter of my name and girl and I like hearts*". When he answered Q2 Session 5 he said "*ObjectPass, the reason: I think better*". So his answer in the first instance provided a fully understanding of what he meant by "better".

7.3 Results and Discussion

The comparison between DoodlePass and ObjectPass authentication systems were based on three usability aspects: effectiveness, efficiency, and satisfaction.

The first section will present the results on effectiveness (measured by accuracy: selection of the correct doodle/object on the first attempt or subsequent attempts) and efficiency (measured by time taken to login; mean times for all attempts) for both systems, and the second section will present the results on satisfaction (measured by children's preferences for DoodlePass or ObjectPass and which they think is more memorable).

7.3.1 Comparison of DoodlePass and ObjectPass authentication systems on effectiveness and efficiency

In this section the comparison will be as follows: first, to measure accuracy and time by the use of two-way repeated measures ANOVA (PassType x Login) for DoodlePass:1 vs ObjectPass:1. Second to measure accuracy and time by the use of two-way repeated measures ANOVA (PassType x Login) for DoodlePass:2 vs ObjectPass:2. Third, to measure accuracy and time by the use of two-way repeated measures ANOVA (PassType x Login), three-way mixed measures ANOVA (PassType x login x Grade) and three-way mixed measures ANOVA (PassType x login x Preference for DoodlePass/ObjectPass) for DoodlePass:3 vs ObjectPass:3.

7.3.1.1 DoodlePass:1 vs ObjectPass:1

For effectiveness, accuracy for both systems is shown in Table 6.2. A two-way repeated measures ANOVA showed that ObjectPass:1 is significantly more accurate than DoodlePass:1, with a large effect size (PassType: $F(1,20) = 5.09$, $p = 0.035$, $\eta^2 = 0.21$). There was no

significant effect due to Login (Login: F (1.51, 30.16) = 2.13, n.s., $\eta^2 = 0.09$) nor was there a significant interaction between PassType and Login (F (1.51, 30.16) = 2.13, n.s., $\eta^2 = 0.09$).

Table 7.2 Accuracy of DoodlePass1 and ObjectPass:1 (mean number of attempts required)

PassType	Session 1, Login 1	Session 1, Login 2	Session 2, Login 1	Session 2, Login 2	Total
DoodlePass1	1.00	1.10	1.05	1.29	1.11
ObjectPass1	1.00	1.00	1.00	1.00	1.00
Both passes	1.00	1.05	1.03	1.15	

For efficiency, login time for both systems is shown in Table 6.3. These mean times are also illustrated in Figure 6.1. A two-way repeated measures ANOVA showed no significant difference between DoodlePass:1 and ObjectPass:1 (PassType: F (1,18) = 2.14, n.s., $\eta^2 = 0.11$). There was also no significant effect due to Login (F (2.71, 48.74) = 0.49, n.s., $\eta^2 = 0.27$) and no significant interaction between PassType and Login (F (2.55, 45.92) = 0.42, n.s., $\eta^2 = 0.023$).

Table 7.3 Mean Login times (and standard deviations) for DoodlePass:1 and ObjectPass:1*

PassType	Session 1, Login 1		Session 1, Login 2		Session 2, Login 1		Session 2, Login 2		Total Mean
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	
DoodlePass:1	12.51	7.51	10.77	7.86	11.93	6.92	11.81	16.73	11.76
ObjectPass:1	11.14	5.87	9.76	6.63	10.43	3.66	9.81	5.50	10.29
Both passes	11.82	6.69	10.27	7.20	11.18	5.52	10.81	6.32	11.02

* Session 2, Login 2 had two very long times (57.17 and 67.57), more than twice as long as the next longest time – 27.35; so I omitted those two participants for this analysis.

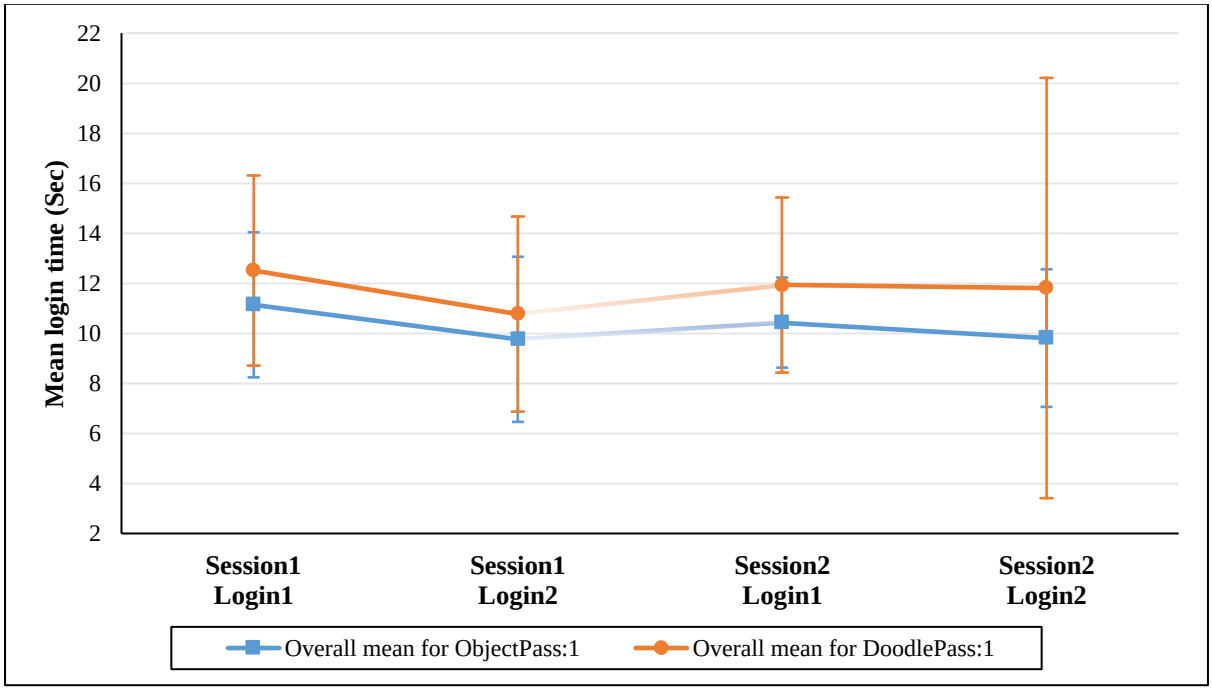


Figure 7.1 Mean login times (and standard deviations) for all attempts in DoodlePass:1 vs ObjectPass:1
Note: Shaded line indicates the one week gap (Medium Term Recognition) between Session1 and Session2

7.3.1.2 DoodlePass:2 vs ObjectPass:2

For effectiveness, accuracy for both systems is shown in Table 6.4. A two-way repeated measures ANOVA showed no significant difference between DoodlePass:2 and ObjectPass:2 (PassType: F (1,20) = 0.32, n.s., η^2 = 0.016). There was also no effect for Login (F (1.12, 22.38) = 0.49, n.s., η^2 = 0.024) and no significant interaction between PassType and Login (F (1.15, 23.02) = 1.18, n.s., η^2 = 0.056).

Table 7.4 Accuracy of DoodlePass:2 and ObjectPass:2

PassType	Session 2, Login 3	Session 3, Login 1	Session 3, Login 2	Total
DoodlePass:2	2.05	2.05	2.10	2.07
ObjectPass:2	2.00	2.10	2.00	2.03
Both Passes	2.025	2.075	2.05	

For efficiency, login times for both systems is shown in Table 6.5. These mean times are also illustrated in Figure 6.2. A two-way repeated measures ANOVA showed no significant difference between DoodlePass:2 and ObjectPass:2 (PassType: F (1,20) = 4.13, n.s., η^2 = 0.17). There was a significant effect due to Login with a large effect size (F (1.35, 26.95) = 15.01, p

< 0.001, $\eta^2 = 0.429$) but no interaction between PassType and Login (F (1.69, 33.87) = 1.80, n.s., $\eta^2 = 0.083$). Regarding the main effect for Login (see Figure 4.2 in Chapter 4, section 4.2.1 for login distribution in each session), follow up post hoc comparisons (Bonferroni) showed that Session 3, Login 1 is significantly longer than Session 2, Login 3 ($p < 0.006$), meaning the one week gap (medium term recognition) has an effect on login times. Moreover, Session 3, Login 1 is significantly longer than Session 3, Login 2 ($p < 0.001$), meaning even a 10 minute gap (short term recognition) has an effect. Session 2, Login 3 is not significantly different from Session 3, Login 2. In summary, at the beginning of Session 3, the login is significantly longer, but then returns to the level of the previous session.

Table 7.5 Mean login times (and standard deviations) for DoodlePass:2 and ObjectPass:2

PassType	Session 2, Login 3		Session 3, Login 1		Session 3, Login 2		Total Mean
	Mean	SD	Mean	SD	Mean	SD	
DoodlePass:2	20.41	6.42	23.41	9.41	20.11	7.33	21.31
ObjectPass:2	16.29	5.40	23.57	11.25	15.19	4.23	18.35
Both Passes	18.35	6.22	23.49	10.24	17.65	6.41	19.83

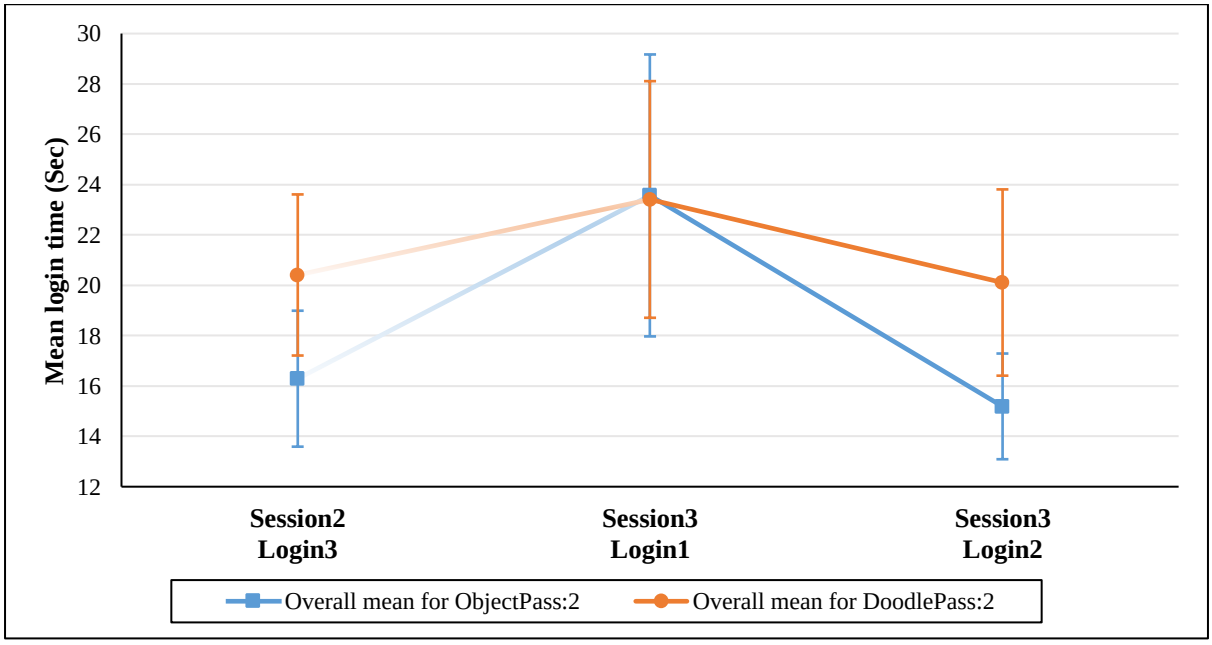


Figure 7.2 Mean login times (and standard deviations) for all attempts in DoodlePass:2 vs ObjectPass:2

7.3.1.3 DoodlePass:3 vs ObjectPass:3

For effectiveness, accuracy for both systems is shown in Table 6.6. A two-way repeated measures ANOVA showed that ObjectPass:3 is significantly more accurate than DoodlePass:3 with a large effect size (PassType: F (1,19) = 12.73, p = 0.002, η^2 = 0.40). There was also a significant effect for Login also with a large effect size (F (2.24, 42.46) = 11.26, p < 0.001, η^2 = 0.372) but no interaction between PassType and Login (F (2.06, 39.09) = 2.65, n.s., η^2 = 0.12). For the main effect for Login, follow up post hoc comparisons (Bonferroni) showed that: Session 5, Login 1 is significantly longer than Session 3, Login 3 (p = 0.001), Session 5, Login 1 is significantly longer than Session 4, Login 1 (p = 0.003), and Session 5, Login 1 is significantly longer than Session 4, Login 2 (p = 0.005). However, Session 5, Login 1 and Session 5, Login 2 are not significantly different, neither are all the logins in Session 3 and Session 4 and neither is Session 5, Login 2 significantly different from all the times in Session 3 and Session 4, so it is only Session5-Login1 that is significantly longer.

Table 7.6 Accuracy of DoodlePass:3 and ObjectPass:3*

PassType	Session 3, Login 3	Session 4, Login 1	Session 4, Login 2	Session 5, Login 1	Session 5, Login 2	Total
DoodlePass:3	3.14	3.19	3.29	4.95	4.05	3.72
ObjectPass:3	3.00	3.14	3.00	3.76	3.05	3.19
Both Passes	3.07	3.17	3.15	4.36	3.55	

* In DoodlePass:3, one child did not complete Session 5 so I omitted this participant in this analysis

For efficiency, login times for both systems are shown in Table 6.7. These mean times are also illustrated in Figure 6.3. A two-way repeated measures ANOVA showed that ObjectPass:3 is significantly quicker than DoodlePass:3 with a large effect size (PassType: F (1,16) = 14.53, p = 0.001, η^2 = 0.48). There was also a significant effect for Login with a large effect size (F (2.48, 39.63) = 17.77, p < 0.001, η^2 = 0.53) and a significant interaction between PassType and Login: F (2.39, 38.15) = 3.41, p = 0.036, η2 = 0.17). Regarding the main effect for Login, follow up post hoc comparisons (Bonferroni) showed that Session 4, Login 1 is significantly longer than Session 3, Login 3 (p = 0.02), meaning the one week gap (medium term recognition) has an effect on login times. In addition, Session 5, Login 1 is significantly longer than all the previous times (p < 0.001), showing that a long term gap also has an effect. Furthermore, Session 5, Login 1 is significantly longer than Session 5, Login 2 (p = 0.003), so

once children recognise their doodles or images after the gap of one week (medium term recognition), the process becomes significantly quicker.

For the interaction between PassType and Login, looking at Figure 6.3, the effect is that after the long term recognition the increase in mean login time is much greater for DoodlePass:3 than ObjectPass:3, and although the mean login time decreases with the second login, the difference between DoodlePass:3 and ObjectPass:3 is still much greater than in Session 3 and Session 4.

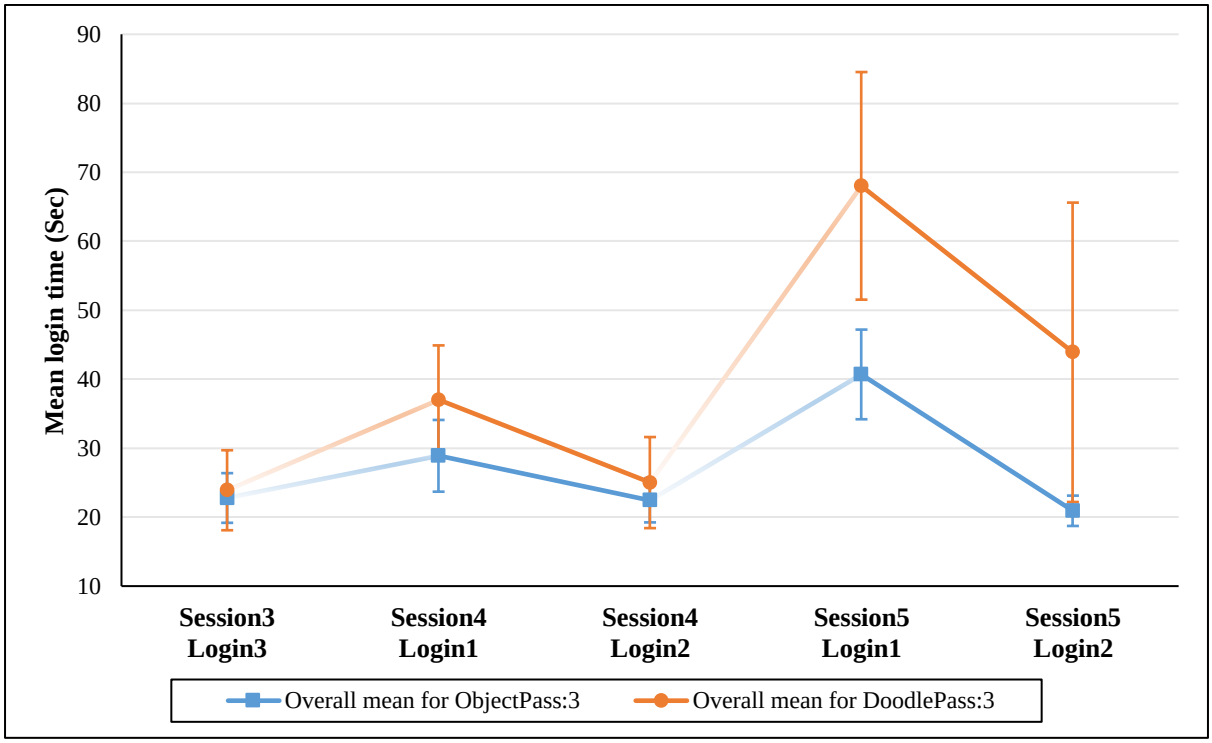


Figure 7.3 Mean login times (and standard deviations) for all attempts in DoodlePass:3 vs ObjectPass:3

Table 7.7 Login times for DoodlePass:3 and ObjectPass:3 across sessions*

PassType	Session3-Login3		Session4-Login1		Session4-Login2		Session5-Login1		Session5-Login2		Total Mean
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD	
DoodlePass:3	23.90	11.51	37.00	15.72	25.01	13.26	68.03	32.97	43.90	43.37	39.57
ObjectPass:3	22.78	7.22	28.89	10.39	22.44	6.35	40.69	13.04	20.92	4.42	27.14
Both Passes	23.34	9.43	32.95	13.09	23.73	9.61	54.20	23.62	32.41	25.39	33.33

* 4 children had extremely long login times on S5-Login1, so were not included. In fact, it means that the effect of the long term gap was even greater.

For DoodlePass:3 and ObjectPass:3 only the effect of children's grade was also investigated, as this was the comparison which showed the most significant differences. For effectiveness, a three-way mixed measures ANOVA was conducted (PassType x Login x Grade), PassType and Login within-participant variables, Grade between-participants variable. This showed no main effect for Grade ($F(1,18) = 2.67$, n.s., $\eta 2 = 0.129$) and no interaction between Grade and other variables (PassType x Grade: $F(1, 18) = .84$, n.s., $\eta 2 = 0.045$; Login x Grade: $F(2.23, 40.16) = 1.10$, n.s., $\eta 2 = 0.058$; PassType x Login x Grade: $F(1.96, 35.23) = .83$, n.s., $\eta 2 = 0.044$).

For efficiency, the three-way mixed measures ANOVA showed a significant main effect for Grade with a large effect size ($F(1, 18) = 6.89$, $p=0.017$, $\eta 2 = 0.277$). The older children were significant faster at login compared with the younger children (Mean login time for Grades 1 - 3: 42.50 seconds; Mean login time for Grades 4 – 6: 25.98 seconds). However, there were no significant interactions between Grade and the other variables (PassType x Grade: $F(1, 18) = 2.77$, n.s, $\eta^2 = 0.134$; Login x Grade: $F(1.87, 33.65) = 2.14$, n.s., $\eta^2 = 0.106$; PassType x Login x Grade: $F(1.98, 35.68) = 1.28$, n.s., $\eta^2 = 0.067$).

In the analysis of DoodlePass:3 and ObjectPass:3 I also investigated whether children were more effective and more efficient with the pass which they said they preferred (see section 6.3.2, for further discussion of this point. 8 children preferred DoodlePass while 12 children preferred ObjectPass, so this was used as a between-participants variable in a three-way mixed measures ANOVA (PassType x Login x Preference). For effectiveness, there was no significant main effect for Preference ($F(1,18) = 0.03$, n.s., $\eta 2 = 0.002$) and no interaction between Preference and the other variables (PassType x Preference: $F(1, 18) = 0.15$, n.s., $\eta 2 = 0.008$; Login x Preference: $F(2.25, 40.56) = 0.33$, n.s., $\eta 2 = 0.018$; PassType x Login x Preference: $F(2.10, 37.76) = 0.61$, n.s., $\eta 2 = 0.033$).

For efficiency, the three-way ANOVA showed no main effect due to preference (Preference: $F(1,18) = 0.03$, n.s., $\eta 2 = 0.002$). The interactions between Preference and other variables were also not significant (PassType x Preference: $F(1, 18) = 0.00$, n.s., $\eta^2 = 0.000$; Login x Preference: $F(1.72, 31.03) = 0.67$, n.s., $\eta^2 = 0.036$; PassType x Login x Preference: $F(1.88, 33.78) = 0.56$, n.s., $\eta^2 = 0.030$).

7.3.2 Children's preferences for DoodlePass or ObjectPass

Children were asked whether they thought remembering DoodlePass or ObjectPass would be easier (Q1). 8 children said they thought DoodlePass would be easier to remember, 13 children said they thought ObjectPass would be easier. This was not a significant preference for either systems in terms of ease of remembering (chi-square = 1.19, df= 1, p = 0.28). Nor was there any significant trend with grade. As the number of children is small, they were grouped into levels of three grades. Table 6.8 shows the numbers (and percentage) of children at each level. A chi-square showed that the distribution did not differ from random (chi-square = 0.08, df = 1, p= 0.78).

Table 7.8 Preference for DoodlePass or ObjectPass for ease of remembering by children's grade

Grade	1 to 3	4 to 6	Total
ObjectPass	9	4	13
	60%	66.7%	61.9%
DoodlePass	6	2	8
	40%	33.3%	38.1%

A summary of the categories of the answers given to explain their choices is given in Table 6.9. All 21 children provided some kind of explanation of their choice. The most commonly mentioned reasons for thinking ObjectPass will be easier to remember is that the shapes are clear and children think they do not draw shapes well themselves. The most comment reason for thinking DoodlePass will be easier to remember is that the children think they will recognise their own drawing because they draw it themselves.

Approximately half the children (11, 52.4%) only explained why their particular choice was easier to remember, but 8 children (38.1%) made an explicit contrast between the two systems (e.g. P23, G1, who preferred ObjectPass said *"Because I draw things in Doodle[Pass] that I am not used to drawing however in ObjectPass I choose thing that I love"*), and two children (9.5%) only mentioned why they did not prefer the other choice (e.g. P28, G2, who preferred ObjectPass said *"Because the drawings of doodles confused me, I cannot remember [them]*).

Table 7.9 Reasons given for thinking DoodlePass or ObjectPass is easier to remember (N = 21)

Reason	Examples	Frequency
ObjectPass easier to remember because …		**N = 13**
1) Positive points to ObjectPass		
Shapes are clear/ organised/ fixed	ObjectPass has clear shapes (P2, G6)	6 46.2%
The objects are things the child likes/ love	I choose things that I love (P23, G1)	2 15.4%
The objects are things related to the child	I choose things that are more related to me like the first letter of my name, and girl, and I like hearts (P17, G3)	1 7.7%
The objects are more memorabile	Objects more easier to remember and if I draw I might be confused with drawing (P19, G6)	1 7.7%
2) Negative points to DoodlePass		
The child thinks cannot draw well to create doodles/ The child thinks will draw unclear doodles	I do not draw well (P3, G2) If I draw it, the drawing will not be accurate (P10, G5)	6 46.2%
The child did not use DoodlePass for long time/ The child cannot remember DoodlePass	I cannot remember (P28, G2)	2 15.4%
Draw things that is not used to draw it	Because I draw things in doodle that I am not used to draw (P23, G1)	1 7.7%
Doodles are confusing	Because the drew of doodles confused (P28, G2)	1 7.7%
DoodlePass easier to remember because ….		**N = 8**
1) Positive points to DoodlePass		
The child can draw it by himself	Because I drew it by myself (P1, G3)	4 50%
The child chose what to draw	Because I can draw what I like (P5, G3)	2 25%
The child will recognise their own handwriting/ drawing	Because I know my handwriting (P6, G3)	2 25%

Children were also asked which they preferred, DoodlePass or ObjectPass (Q2). Interestingly, two children who said ObjectPass was easier to remember than DoodlePass said they preferred DoodlePass to ObjectPass and one child who said DoodlePass was easier to remember than ObjectPass said they preferred ObjectPass. So, the number of children preferring ObjectPass was 12, compared to 13 who said they thought it was easier to remember. Again, there was a

fairly even split in preferences between the two systems, with 9 children saying they preferred DoodlePass and 12 saying they preferred ObjectPass. Thus, there were no significant trend in the preferences (chi-square = 0.43, df = 1, p=0.51). Nor was there any significant trend with age. As the number of children is small, they were grouped into levels of three grades. Table 6.10 shows the numbers (and percentage) of children at each level. A chi-square showed that the distribution did not differ from random (chi-square = 0.18, df = 1, p = 0.68).

Table 7.10 Preference for DoodlePass and ObjectPass by children's grade

Grade	1 to 3	4 to 6	Total
ObjectPass	9 60%	3 50%	12 57.1%
DoodlePass	6 40%	3 50%	9 42.9%

A summary of the categories of the answers given to explain their choices is given in Table 6.11. All 21 children provided some kind of explanation of their choice. Coding of the answers started with the categories from the ease of remembering question (Table 6.9) and added further categories as needed. Six more categories were needed to describe the preferences for ObjectPass compared to only two categories for DoodlePass. In each case, ease of remembering was added as a category, possibly prompted by the earlier question. Only three categories from the remembering question were not used, that of preferring ObjectPass because the objects are things related to the child, cannot remember doodles, and drawing things that the chid is not used to drawing.

The most commonly mentioned reasons for preferring ObjectPass was a general statement that it was better, that the object shapes are clear, that the child thinks they do not draw well enough to create the doodles or that it will be easier to remember. The most commonly mentioned reasons for preferring DoodlePass were that the child was allowed to draw themselves and to choose what to draw.

Most of the children (15, 71.4%) only mentioned why they thought their choice was more preferred, 3 children (14.3%) made an explicit contrast between the two systems (e.g. P19, G6, who preferred ObjectPass said *"Pictures are clear while in doodles the draw could confuse me as it is not accurate"*), and 3 children (14.3%) only mentioned why they did not prefer the other choice (e.g. P26, G1, who preferred ObjectPass said *"Because I do not like to draw on iPad it will be bad"*).

Table 7.11 Reasons given for preferring DoodlePass or ObjectPass (N = 21) (* = new category from Table 6.9)

Reason	Examples	Frequency
Prefer ObjectPass because …		**N = 12**
1) Positive points to ObjectPass		
General positive statement: good, better, easier*	Easier (P28, G2)	4 33.3%
Shapes are clear	Because it has clear pictures similar to the original pictures (P25, G1)	3 25%
Child will remember the objects	Because it is easy to remember (P14, G5)	2 16.7%
The objects are things the child likes	Because the draw in doodle I did not like it however in object I like it (P23, G1)	1 8.3%
Child does not need to know how to draw*	Because you do not need to know how to draw (P5, G3)	1 8.3%
ObjectPass more organised than DoodlePass*	More organised than doodles (P11, G5)	1 8.3%
Objects are beautiful*	The object is more beautiful (P9, G1)	1 8.3%
2) Negative points to DoodlePass		
The child thinks they do not draw well to create doodles	When I draw I could not have clear picture in doodle (P25, G1)	2 16.7%
They think they might get confused by drawings	In doodles the draw could confuse me as it is not accurate (P19, G6)	1 8.3%
Child did not like their drawings in DoodlePass*	Because the draw in doodle I did not like it however in object I like it (P23, G1)	1 8.3%
Child did not like drawing with iPad*	Because I do not like to draw on iPad it will be bad (P26, G1)	1 8.3%
Prefer DoodlePass because ….		**N = 9**
1) Positive points to DoodlePass		
The child was allowed to draw it themselves	Because I drew it by myself (P1, G3)	4 44.4%
The child chose what to draw	Because I can draw what I like (P13, G1)	3 33.3%
Child likes drawing*	I like drawing (P4, G2)	2 22.2%
The child will recognise their own drawing	Because I know the way I draw (P27, G5)	1 11.1%
Easy to remember*	Because it is easy to remember (P14, G5)	1 11.1%

While having the same participants using the same systems in the same order has an advantage to ensure differences are compared within participants, this also has a main limitation. The main limitation would be the order and practice effects. Participants behaviour might be affected by using both system in the same order. Participants' performance in using the ObjectPass authentication system was better compared with the DoodlePass authentication system. This could be explained by the fact that the experience with DoodlePass gave participants more of an idea what to expect and what to do with the ObjectPass authentication system. To investigate in future work, the performance of participants who only participated in the evaluation of the ObjectPass authentication system should be compared with the performance of participants who took part in the evaluation of both systems.

I planned to conduct such further analyses to compare the two systems in greater detail, but due to time constraints this was not possible. Firstly, further research is needed to analyse and compare the types of errors children made with each system (e.g., a child may have chosen the wrong image but one which belongs to the same category as their image; a child may have chosen the wrong image and one which is not in the same category as their image; or a child may have chosen the images in the wrong order). Unfortunately, this analysis could not be conducted with my current data set as the types of error for Sessions 1 to 4 in evaluation of the DoodlePass authentication system were not recorded. Secondly, further research could analyse the type of images that children chose for ObjectPass and whether they were related to the doodles they had created for DoodlePass, both in term of similarities and the effects of these choices on effectiveness and efficiency when subsequently using the ObjectPass authentication system.

7.4 Conclusions

To conclude, this chapter compared the effectiveness and efficiency of the DoodlePass and ObjectPass authentication systems and children's satisfaction with the systems, using the sample of children who used both the DoodlePass and ObjectPass authentication systems in this programme of research. The results show that the ObjectPass authentication system is more successful in achieving these three usability aspects compared to the DoodlePass authentication system. Although the sample size was not large (21 children), where significant effects were achieved, they were large effect sizes, so robust results. A number of further investigations

can be undertaken with these data in the future. However, result could not be generalised due to small sample of participants and no children at grade 4 participate in this comparison.

Chapter 7

General Discussion and Conclusions

8.1 Introduction

Children in the age range 6 to 12 years, who were born in the 2010s, are part of "Generation Alpha" (Yurtseven, 2020) are important segment of population. This generation are growing up with technology and the idea of changing adult's technologies to be suitable for children, might be not ideal solution (Read & Markopoulos, 2013). In fact, they deserve technologies and products designed specifically for them which meet their needs and capabilities (Dempsey et al., 2016). The literature review presented in Chapter 2 showed that children struggle with text password while little research has explored children knowledge and understanding of digital security and authentication. Additionally, only a few researchers have proposed usable authentication systems for children. Among this research, I could find no research that explores the challenges and needs for children who are native speakers of Arabic.

This programme of research aimed to design and evaluate a usable graphical authentication system suitable for Arab children aged 6 to 12 years, considering their level of cognitive development and literacy skills. To do this, an exploratory study was conducted with Arab children to understand the password knowledge and best practices for children of this age group who are native speakers of Arabic. The results of this exploratory study helped me to design and evaluate two graphical authentication systems for young Arab children.

The overall discussion and conclusions for this programme of research are presented in this chapter. The structure of this chapter is as follows: an overview of each study and their outcomes in relation to their research questions. Then, the overall contributions of the programme of research, and lessons learned from the programme of research. Finally, the chapter concludes with limitations of the research and suggestions for future work.

8.2 Overview of the Programme of Research

The main research question for the programme of research is, *Are graphical authentication systems usable and acceptable for young Arab children?* To answer this research question, this research was divided into three main phases:

Phase 1. Comprised Study 1 (Chapter 3), which aimed to answer the following research questions:

RQ1: Do Saudi children use digital devices at home or at school?

RQ2: Do Saudi children understand the reasons for having passwords and how to create good ones?

RQ3: Do Saudi children have linguistic problems in relation to password creation in the Latin alphabet and in English?

RQ4: At what age do Saudi parents think it is important for their children to understand how to make passwords for online systems?

In this phase the study aimed to investigate 39 Saudi children's aged 6 to 12 years, their practices, perceptions, and knowledge regarding text passwords. The answers for this interview were gathered from both children and their parents to get accurate answers as each of them had to answer specific questions, but could also help with answers to the other person. The results of this study showed that all children used at least one digital device and nearly three quarters (74.4%) of children had at least one password. The children had a good understanding of security best practices but when it comes to create an easy and hard password, they could not apply these practices. It is clear from the results that Arabic children struggle due to lack of academic curriculum at schools and their literacy in the English language. On the other hand, parents are doing their best to educate their children and support them about security practices, more than half of the parents in this study (59%) think it is important to educate children about security best practices and almost all (80%) know their child's password and login to keep track of their activities. Therefore, it was important to investigate age-appropriate authentication systems, which was presented in the next studies.

Phase 2. Comprised Study 2 (Chapter 4) and Study 3 (Chapter 5), which aimed to answer the following research questions:

RQ5: Is the DoodlePass authentication system usable by children aged 6 to 12 years?

RQ6: Why do children think they need a password? (investigated again with different participants in this study)

RQ7: Is the ObjectPass authentication system usable by children aged 6 to 13 years?

As reported in the previous phase of research, literacy and memorability were common challenges for children while using text password. In this phase two graphical authentication systems: DoodlePass and ObjectPass authentication, were developed and evaluated according to three usability aspects: effectiveness, efficiency, and satisfaction. Both systems took advantage of the fact that they depend on recognition of pictures rather than recall of alphanumeric characters. The DoodlePass authentication system was evaluated with 37 Saudi children ages 6 to 12 years. The children created their own drawings (doodles) and then used them in the authentication system. Due to the time consuming nature of having children make their own drawings and the process to add them to the system, as well as some feedback regarding lack of proficiency or preference at drawing, I decided to improve the authentication system by replacing the doodles to be images of objects. This improvement resulted in the ObjectPass authentication system, and this system was evaluated with 52 Saudi children ages 6-13 years.

The results for both systems were promising, effectiveness was shown by the very high accuracy rate. For the DoodlePass authentication system 98.5% of the children recognised and selected their DoodlePass, while all children recognised and selected their ObjectPass. For efficiency, the times taken to login in for both systems were reasonable. In terms of satisfaction, most children preferred DoodlePass or ObjectPass in comparison to a text password. Furthermore, a majority of children thought that ObjectPass was easier to remember than a text password, while for DoodlePass children answers varied between DoodlePass and text password. These results encouraged further analysis to compare the three usability aspects between the two systems, which was presented in the next phase.

Children demonstrated a general understanding of the purpose for using passwords. Mostly they want to avoid other's actions (67.3%), with preventing unauthorised access having the highest percentage among children's answers (70.2%). Overall children's greatest understanding is to prevent access to their devices (61.4%). It is interesting to note that about a third of the children (30.7%) used security words in their answers (e.g., privacy, hack). Most used security words were from older children. However, it may be that younger children here are expressing the same ideas, but they are using more concrete ways of describing privacy and security, as they have not reached the stage in their development that involves abstract thinking and concepts (the formal operational stage) and thus have not understood learnt these concepts and terms in abstract terms yet.

Phase 3. Comprised Study 4 (Chapter 6), which aimed to answer the following research questions:

RQ8: Which system was more usable, the DoodlePass authentication system or the ObjectPass authentication system?

RQ9: Does the children's age affect their performance and attitudes towards the DoodlePass authentication system and the ObjectPass authentication system?

In this phase, a further set of analyses was conducted to compare both systems in term of three usability aspects: effectiveness, efficiency, and satisfaction. 21 children aged 6 to 12 years had participated in both Studies 2 and 3, meaning they had used both systems. The results of these analyses showed that the ObjectPass authentication system was more successful in achieving these three usability aspects compared to the DoodlePass authentication system. In addition, in term of effect of children's age, the older children were significant faster at login compared with the younger children.

8.3 Contributions of the Programme of Research

Considering all the research discussed in this programme of research, to the best of my knowledge this is the first time Arab children have been involved in theoretical and empirical research in the field of usable authentication system for children. No previous research with Arab children was found for the literature review (see Chapter 2). All the studies conducted in

this programme of research help to understand the importance of having a usable authentication system for children.

The specific contributions of the studies are:

The first contribution is the development of an understanding of Arab children's (aged 6-12 years) knowledge about security and best practices in relation to text passwords. In this work the parents of children were also involved in answering questions, which gives more strength and accurate answers to the interview questions. In the literature review (Assal et al., 2018; Hundlani et al., 2017; Maqsood et al., 2018) it has been reported that parents have a significant role in children's knowledge development. As far as I am aware, only one study involved parents in their work on this topic (Ratakonda et al., 2019). Additionally, as far as I am aware, this was the first such study on this topic that involves children whose first language is Arabic.

The second contribution is the design, implementation, and evaluation of two graphical authentication systems suitable for children aged 6 to 12 years, DoodlePass and ObjectPass authentication systems. The first system uses children's own drawings and the second system uses images of objects. Both systems were designed in two interfaces: one with the English language and the another with the Arabic language. To the best of my knowledge, this is the first time a graphical authentication system for children is designed with an Arabic language interface. Both authentication systems were evaluated with young Arabic speaking children, aged 6-12 years. This evaluation showed that both systems are effective, efficient and promising alternative to text passwords to overcome the literacy and memorability challenges for Arabic speaking children in this age group. The graphical systems in this programme of research, the DoodlePass and ObjectPass authentication systems, were compared in some detail. The results showed that ObjectPass is significantly more effective, efficient, and satisfying than the DoodlePass authentication system.

8.4 Limitations and Future Work

The programme of research achieved a number of contributions to the field of authentication systems for children and usable security for children that are summarised above in this chapter. However, it is important to highlight limitations identified in conducting the studies and suggest future work to address these limitations and other issues which I could not investigate.

Overall, children can be unreliable informants and can sometimes not be very full in their answers. In some cases for the interview questions in Study 1 (Chapter3) and the pre- and post-questions in Study2 (Chapter 4) and Study 3 (Chapter 5), if I had realized this, I would added follow up- questions and probed the children more to clarify exactly what they meant and why they had said something different in a different question. In addition, the open ended questions in the programme research had the same language and format for all age groups. However, in some cases, the younger children found it difficult to answer open ended question, it would have been better to make the format and language of questions more appropriate for each age group, and have different questions for younger and older children. This is recommended for future research.

For Study 1 (Chapter 3), the comparison between the two different type of schools (stated-funded schools and privately-funded schools) to understand language literacy did not reveal any significant differences. The issue could be the English curriculum in privately-funded schools which is not intensive as I thought. Although at the beginning of this study it was planned to conduct this study with children from Saudi Arabia and UK, however, due to the mode of my study (distance learning) this goal could not achieved. For future work it would be very interesting to compare the results that I have obtained with results from native English speaking children or Arab children attending a private international school whose English will be better. Other limitation of this study was that demographic information about the parents interviewed was not collected. This information could be important when studying the role of parent with their children regarding password and security best practices.

For the graphical authentication systems, although few children selected their images in the wrong order, it would be very interesting to investigate what strategies, if any, children follow to enable them to recognize their authentication keys in the correct order. Furthermore, it would be interesting to investigate if certain categories of types of images (e.g., drawings, photos, colour photos or black and white photos) and the objects represented in the images are easier for children to recognise than others.

The results for both graphical authentication systems show their usability when evaluated with Saudi children, however, to generalise the results, those two systems need to be evaluated with children from other countries, particularly those with different cultures and language from Saudi Arabia.

There are three main elements which are worth investigating in the future, however they were beyond the capacity of this programme of research. Firstly, authentication credentials typically consist of both a username and a password. In this programme of research the children's passwords were the focus of research. This work could be further developed by investigating usernames and the usability of having graphical usernames for children. Secondly, authentication systems rely on a balance between usability and security. In this programme of research the focus was on usability, this work could be further developed by looking at the authentication systems more from a security preceptive as well. For example, looking at the theoretical password spaces for these graphical systems (entropy), investigating the type of security threats that both systems are prone to, for example brute force attacks, guessing attacks, and shoulder surfing attacks. Thirdly, using the same graphical authentication system for more than one accounts to test its usability for both short and long term has not yet investigated in the literature presented at this thesis. Thus, it is worth, for example, to evaluation the performance of children when they have deal with more than one DoodlePass or ObjectPass account.

8.5 Conclusions

Children interact with digital technologies on a daily basis, these technologies regularly demand the use of authentication systems to access devices or accounts. Children are still developing their cognitive skills, therefore, they should not be required to be experts as adults when using these authentication systems. This programme of research aimed to evaluate the usability of graphical authentication systems for children. To achieve this goal, young Arab children's knowledge and understanding was investigated carefully to be aware of their challenges and their cognitive abilities. The results were promising, both the graphical authentication systems developed and evaluated in this programme of research are effective and efficient, and promising alternatives for text passwords to overcome literacy and memorability challenges for Arab children in this age group.

Appendix A

A.1: Improvements in the interview schedule as a result of the pilot study

Q	Questions in the preliminary version	Questions in the final version	Reason of changing or adding
1	Child age: ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12	No change in this question but I added the question: 5. Child grade (last grade completed): ○ Grade 1 ○ Grade 2 ○ Grade 3 ○ Grade 4 ○ Grade 5 ○ Grade 6	To be more accurate about the child's level of education
2	Have you used a computer?	13. Does your child use the Internet/the Web by themselves? 14. Does your child have any accounts on the Internet/Web themselves? 8. What digital devices does your child use at home? 9. What does your child use these for? 16. What digital devices does your child use at school (you may need to check with them)?	I need to understand more the type of devices that children use
3	Have you ever had to use a password to log into a computer or website?	10. Do any of the digital devices your child uses at home need a password/passcode to open? 17. Do any of the digital devices your child uses at school need a password/passcode to open? 15. Do any of these accounts need passwords?	Question needed to be divided to more specific sub questions

Q	Questions in the preliminary version	Questions in the final version	Reason of changing or adding
4	In your opinion, what makes a good password? ☐ Simple ☐ Easy to remember ☐ Hard to guess ☐ Name of a pet ☐ Letters and Numbers ☐ Has an easy clue ☐ Easy to forget ☐ Easy to copy	27. In your opinion, what makes a good password? ☐ Simple ☐ Easy to remember ☐ Hard to guess ☐ Name of famous person (e.g., celebrity, football team) ☐ Letters and Numbers ☐ Has an easy clue ☐ Easy to forget ☐ Easy to copy	We do not have a lot of interest in pets in Saudi Arabia
5	Why do people put passwords in computer games and things?	25. Why do people have passwords?	I make it more in general as old question related to passwords in computer where children might have password for online accounts
6	Can you give an example in each box below of a computer (or website) password that would be very easy to guess and example of a strong (hard to guess) password? (Please do not use your own password)	No change in this question but I add two more questions related to this question: 29. Why was that an easy password? 30. Why was that a strong/hard password?	It was unclear in the old question why they decide those passwords to be easy or hard.
7	Why do you think that strong computer (or website) passwords are used in real life?	26. Why do you think that strong passwords are used in real life?	I make it more in general and to be consistent with other questions in the interview

Q	Questions in the preliminary version	Questions in the final version	Reason of changing or adding
8	Do you know the meaning of threats? If YES, list all type of threats that you know.	-	Advance wording for children in elementary school
9	How many English words the child knows?	22. How many English words does your child know?	Edit question wording
10	Have you ever had to make up a computer (or website) password?	12. Have your child ever had to change his password at home? 19. Have your child ever had to change his password at school?	Question needed to be divided to more specific sub questions
11	How many passwords do you have?	24. About how many passwords do you have?	Edit question wording
-	-	1. Who did this interview? (parent, aunt, ...) 2. Profession of the person who fill this survey? (Bachelor, Master, or PhD in .....) 3. Parent email: _____	Newly added questions which aimed to gather details about who did this interview
-	-	7. Type of school? o Private (Private school in Saudi Arabia means privately-funded school in UK) o Public (Public school in Saudi Arabia means State funded school in UK)	Newly added question aimed to know child level of English language which depends on school type

Q	Questions in the preliminary version	Questions in the final version	Reason of changing or adding
-	-	11. What is the structure of each of the passwords/passcode they have at home? (First entry is an example for you) 18. What is the structure of each of the passwords/passcode they have at school "if your child knows this information"? (First entry is an example for you)	Newly added questions to understand the natural of passwords chosen by child in Q6 in this table
-	-	20. Do you login yourself with passwords to systems that your child uses? 21. Do you create passwords for your child to use for online systems?	Newly added questions to understand child ability to manage his password by his own
-	-	23. Do you think it is important for your child to understand about making passwords for online systems at their age?	Newly added question to understand how much parents care about teaching their children about password creation

A.2: Interview schedule for Study 1

Children's understanding of online security and passwords

Thank you for offering to take part in this study. I'm Esra Khalil Alkhamis. It is part of my PhD research to create better online security and password creation systems for children.

In this study, I would like to ask your child some simple questions about their understanding of online security and passwords and ask them to make a good and a bad password. I don't want them to use any passwords they may currently have, so I won't compromise security of any of their accounts. I would also like to ask you several questions about your child's use of passwords.

Any information you and your child provide will be completely confidential and stored securely. If it is used in any public document (reports, journal papers), it will be reported in anonymised manner to protect your identities.

If you or your child feel uncomfortable at any point, you are completely free to withdraw from the study. If you or your child do not wish to answer particular questions, you are completely free to not answer.

I give my consent to participate in this study concerning children's understanding of online security and passwords. I have been informed about and feel that I understand the basic nature of the project. I understand that I or my child may withdraw from the study at any time without prejudice.

- agree

1. Who did this survey? (parent, aunt, ...)

_____

2. Profession of the person who fill this survey? (Bachelor, Master, or PhD in .....)

_____

3. Parent email: _____

4. Child age?

- 6
- 7
- 8
- 9
- 10
- 11
- 12

5. Child grade (last grade completed)?

- Grade 1
- Grade 2
- Grade 3
- Grade 4
- Grade 5
- Grade 6

6. Child gender?

- Male
- Female

7. Type of school?

- Private
- Public

Parents' questions

8. What digital devices does your child use at home?

- ☐ Desktop computer
- ☐ Laptop computer
- ☐ Game console
- ☐ Mobile phone
- ☐ Tablet computer
- ☐ Other (please specify) ……

9. What does your child use these for?

- ☐ Games
- ☐ Entertainment
- ☐ Internet/web
- ☐ School
- ☐ Texting
- ☐ Social media
- ☐ Email
- ☐ Homework
- ☐ Other (please specify) ……

10. Do any of the digital devices your child uses at home need a password/passcode to open?

- o Yes
- o No

11. What is the structure of each of the passwords/passcode they have at home? (First entry is an example for you)

Device type	Password/passcode structure
Ipad	Passcode size should be 4 digits and includes only numbers

12. Has your child ever had to change his password at home?

- o Yes
- o No

13. Does your child use the Internet/the Web by themselves?

- o Yes
- o No

14. Does your child have any accounts on the Internet/Web themselves?

- o Yes
- o No

15. Do any of these accounts need passwords?

- o Yes
- o No

16. What digital devices does your child use at school (you may need to check with them)?

- ☐ Desktop computer
- ☐ Laptop computer
- ☐ Game console
- ☐ Mobile phone
- ☐ Tablet computer
- ☐ Other (please specify) ……

17. Do any of the digital devices your child uses at school need a password/passcode to open?

- o Yes
- o No

18. What is the structure of each of the passwords/passcode they have at school "if your child knows this information"? (First entry is an example for you)

Device type	Password/passcode structure
Ipad	Passcode size should be 4 digits and includes only numbers

19. Has your child ever had to change his password at school?

- Yes
- No

20. Do you login yourself with passwords to systems that your child uses?

- Yes
- No

21. Do you create passwords for your child to use for online systems?

- Yes
- No

22. How many English words does your child know?

23. Do you think it is important for your child to understand about making passwords for online systems at their age?

- Yes
- No

Children's questions

24. About how many passwords do you have?

_____

25. Why do people have passwords?

_____

26. Why do you think that strong passwords are used in real life?

_____

27. In your opinion, what makes a good password?

- ☐ Simple
- ☐ Easy to remember
- ☐ Hard to guess
- ☐ Name of famous person (e.g., celebrity, football team)
- ☐ Letters and Numbers
- ☐ Has an easy clue
- ☐ Easy to forget
- ☐ Easy to copy
- ☐ Other (please specify) ……..

28. Can you give an example in each box below of a computer (or website) password that would be very easy to guess and example of a strong (hard to guess) password? (Please do not use your own password)

Easy password _____

Strong (Hard) password _____

29. Why was that an easy password?

_____

30. Why was that a strong/hard password?

_____

A.3: Interviewer demographic information

Interviewer ID	Gender	Age	Qualification	Number of interviews
1	Female	33	MSc Information System	4
2	Female	38	PhD Computer Science	1
3	Female	32	BA Information Technology	1
4	Female	35	MSc Information System	1
5	Female	32	MSc Computer Science	4
6	Female	32	MSc Information system	6
7	Female	33	BA Information Technology	2
8	Female	36	MSc Computer Science	1
9	Female	32	MSc Computer Science	2
10	Female	33	PhD Computer Science	2
11	Female	36	MSc Computer Science	2

A.4 Different between schools' curricula in term of English and Computer subjects at Saudi Arabia at the time of conducting studies (2018 - early 2020)

Subjects	Stated-Funded School	Privately-Funded School	Private International School
Computer subject	Children do not study Computer at school.	• Start studying Computer in Grade 1 (approximately 6 - 7 years of age) • Computer curriculum is different for each school. • The main focus on computer applications and programming. However, it does not have any content with regard to security aspects and best practices. • Children have access to computer labs	• Start studying Computer in Grade 1 (approximately 6 - 7 years of age) • Computer curriculum is different for each school. • The main focus on computer applications and programming. However, it does not have any content with regard to security aspects and best practices. • Children have access to computer labs
English subject	• Start studying English in Grade 4 (approximately 9 -10 years of age). • English curriculum is based on basic information.	• Start studying English in Grade 1 (approximately 6 - 7 years of age). • English curriculum is more intensive than in stated funded school.	• Start studying English in Grade 1 (approximately 6 - 7 years of age). • English curriculum is more intensive than in private funded school. • Children study most subjects (English, Math, Science, and Social studies) following British or American curriculum.

Appendix B

B.1 DoodlePass authentication system procedure for the other researcher

Student ID:

Student name (first name only):

Student grade:

Student gender:

Type of school:

Pre-session

1) draw 3 doodles using iPad.
2) Date of the draw: ……/……/……
3) Name of the doodles:
    a. Doodle1: ……
    b. Doodle2: ……
    c. Doodle3: ……

Session 1

1) Date: ……/……. /…….
2) Pre questions:
    a. Do you have any passwords?
        - o Yes
        - o No
    b. Why do you think you need passwords?
3) Let child access the website.
    a. Index.php
    b. Game **(he/she has only 10 Minutes)**:

        Time of start: Time of finish:

    c. Index1.php

4) Post questions:
    a. Which do you think is easy to remember:
        - Text password OR
        - DoodlePass
    b. Which do you prefer more:
        - Text password OR
        - DoodlePass

Session 2

1) Date: ……/……. /…….
2) Let child access the website.

    a. Index.php
    b. Game **(he/she has only 10 Minutes)**:
        Time of start: Time of finish:
    c. Index1.php

3) Post questions:

    a. What type of digital devices do you use (Smart TV, PlayStation, iPad, Mobile, … etc)?
    b. Do you use a password to access (each device from previous question)?
        - Yes
        - No
    c. Do you have any password for online accounts?
        - Yes
        - No

Session 3

1) Date: ……/……. /…….

4) Let child access the website.

    a. Index.php
    b. Game **(he/she has only 10 Minutes)**:
        Time of start: Time of finish:
    c. Index1.php

Session 4

1) Date: ……/……. /…….
2) Pre questions:
    a. Do you think remembering three doodles for the DoodlePass much harder than two doodles?
        - o Yes
        - o No
    b. Do you think you would be able to remember three doodles as a DoodlePass for a long time?
        - o Yes
        - o No
3) Let child access the website.

    a. Index.php
    b. Game **(he/she has only 10 Minutes)**:

        Time of start: Time of finish:

    c. Index1.php

Session 5

1) Date: ……/……. /…….
2) Pre questions:
    a. Did you find it easy or hard to remember your DoodlePass?
        - o Yes
        - o No
    b. How did you remember your DoodlePass?
    c. Which one is easier to you to remember:
        - o Text password OR
        - o DoodlePass
    d. Which one did you prefer more:
        - o Text password OR
        - o DoodlePass
3) Let child access the website.

    a. Index.php
    b. Game **(he/she has only 10 Minutes)**:

        Time of start: Time of finish:

    c. Index1.php

B.2 Parent consent letter for DoodlePass authentication system

Dear respected parent,

Esra Alkhamis is a researcher interested in studies related to children in Saudi Arabia as a part of her PhD study.

The aim of the study is to find a secure authentication system for children to be used in accounts and devices as an alternative to regular password.

She will ask child to draw doodles from his/her choice and then every week the child will use these doodles to login to a website built by the researcher with total of 6 weeks.

The study will be done inside the school and we will ensure that child will not be distracted from his/her classes as the meeting will be at the art lesson.

Please note that this study is approved by the University of York in the United Kingdom and all data will be secure and only used for scientific purpose. Each child will receive a voucher from Jarir Bookstore worth 50 SR after completing the study.

For more information and suggestions, you can contact the researcher on:

Ea921@york.ac.uk

Parent approval:

- **Yes**
- **No**

Child name: _____

Class: _____

B.3 Games available for children to play in DoodlePass authentication system

Game name	Type	Link
Chow time	Balance	https://pbskids.org/dinosaurtrain/games/chowtime.html
Dinosaur dive	Balance	https://pbskids.org/dinosaurtrain/games/dinosaurdive.html
Leaf leader	Balance	https://pbskids.org/dinosaurtrain/games/leafleader.html
Buddy's big campout adventure	Collecting specific things	https://pbskids.org/dinosaurtrain/games/campoutadventure.html
Dinocar designer	Design	https://pbskids.org/dinosaurtrain/games/dinocardesigner.html
Track star	Design	https://pbskids.org/dinosaurtrain/games/trackstars.html
Fossil finder	Finding	https://pbskids.org/dinosaurtrain/games/fossilfinder.html
Buddy's amazing adventure	Maze	https://pbskids.org/dinosaurtrain/games/buddysamazingadventure.html
Corn Maze Craze	Maze	https://pbskids.org/catinthehat/games/corn-maze-craze
Moonlight maze	Maze	https://pbskids.org/arthur/games/moonlight-mazes
Bridge builder	Measure distance	https://pbskids.org/dinosaurtrain/games/bridgebuilder.html
Dino Drink	Measure sizes'	https://pbskids.org/dinosaurtrain/games/hydrationstation.html
Pinecone pass	Measure distance	https://pbskids.org/dinosaurtrain/games/pineconepass.html
Roarin' Relay	Measure sizes'	https://pbskids.org/dinosaurtrain/games/roarinrelay.html
Rail rally	Race	https://pbskids.org/dinosaurtrain/games/railrally.html
Station race	Race	https://pbskids.org/dinosaurtrain/games/stationrace.html
All star sorting	Sorting	https://pbskids.org/dinosaurtrain/games/allstarsorting.html
Opening ceremony	Sorting	https://pbskids.org/dinosaurtrain/games/openingceremony.html

Appendix C

C.1 Parent consent letter for ObjectPass authentication system

Dear respected parent,

I am Esra Alkhamis a researcher interested in studies related to children in Saudi Arabia as a part of her PhD study.

The aim of the study is to find a secure authentication system for children to be used in accounts and devices as an alternative to regular password.

I will ask child to choose objects from a set and then every week the child will use these objects to login to a website built by the researcher with total of 5 weeks.

The study will be done online through Zoom at any time suitable to your child to ensure child safety during the COVID-19 pandemic.

Please note that this study is approved by the University of York in the United Kingdom and all data will be secure and only used for scientific purpose. Each child will receive a voucher from Jarir Bookstore worth 50 SR after completing the study.

For more information and suggestions, you can contact the researcher on:

Ea921@york.ac.uk

Parent approval:

- **Yes**
- **No**

Child name: _____

Class: _____

C.2 Study 3 Devices used in each session by children

Child ID	Used device by children in each session				
	Session 1	**Session 2**	**Session 3**	**Session 4**	**Session 5**
1	laptop	Tablet computer	laptop	laptop	laptop
2	Tablet computer	Tablet computer	Tablet computer	Smartphone	Smartphone
3	laptop	Tablet computer	laptop	Tablet computer	Tablet computer
4	Tablet computer	Tablet computer	Tablet computer	Tablet computer	Smartphone
5	Personal computer	Personal computer	laptop	Personal computer	Personal computer
6	laptop	laptop	laptop	laptop	laptop
7	laptop	laptop	laptop	laptop	laptop
8	Smartphone	laptop	laptop	laptop	Tablet computer
9	Smartphone	Tablet computer	Smartphone	Tablet computer	Smartphone
10	Tablet computer	laptop	Smartphone	Smartphone	Smartphone
11	Tablet computer	Tablet computer	Tablet computer	Tablet computer	Smartphone
12	Smartphone	Smartphone	Tablet computer	Tablet computer	Tablet computer
13	Tablet computer	Tablet computer	Tablet computer	Tablet computer	Tablet computer
14	Tablet computer	Smartphone	Smartphone	Smartphone	Smartphone
15	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
16	laptop	laptop	laptop	laptop	laptop
17	laptop	laptop	laptop	laptop	laptop
18	Smartphone	laptop	laptop	Smartphone	laptop
19	Smartphone	laptop	laptop	laptop	Smartphone
20	laptop	laptop	laptop	Smartphone	laptop
21	laptop	laptop	laptop	Smartphone	laptop
22	computer	laptop	laptop	laptop	laptop
23	Tablet computer	Tablet computer	Tablet computer	Tablet computer	Tablet computer
24	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
25	Personal computer	Personal computer	laptop	Personal computer	Personal computer
26	laptop	laptop	laptop	laptop	laptop

Child ID	Used device by children in each session				
	Session 1	**Session 2**	**Session 3**	**Session 4**	**Session 5**
27	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
28	laptop	laptop	Tablet computer	laptop	laptop
29	Personal computer	Personal computer	Personal computer	Personal computer	Personal computer
30	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
31	Tablet computer	Tablet computer	Tablet computer	Tablet computer	Smartphone
32	laptop	laptop	laptop	laptop	laptop
33	laptop	laptop	laptop	laptop	laptop
34	laptop	laptop	Smartphone	Smartphone	Smartphone
35	Personal computer	Personal computer	Personal computer	Personal computer	Personal computer
36	Smartphone	Tablet computer	Smartphone	Tablet computer	Tablet computer
37	Smartphone	Tablet computer	Tablet computer	Tablet computer	Tablet computer
38	Tablet computer	Tablet computer	Tablet computer	Tablet computer	laptop
39	Smartphone	Smartphone	Smartphone	Tablet computer	Tablet computer
40	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
41	laptop	Smartphone	Smartphone	Smartphone	Smartphone
42	laptop	laptop	Tablet computer	laptop	laptop
43	laptop	laptop	Tablet computer	laptop	laptop
44	laptop	laptop	Personal computer	laptop	laptop
45	laptop	laptop	laptop	laptop	laptop
46	Smartphone	Smartphone	Smartphone	Smartphone	Smartphone
47	Tablet computer	Tablet computer	laptop	Tablet computer	Tablet computer
48	laptop	laptop	laptop	laptop	Smartphone
49	laptop	laptop	laptop	Tablet computer	Tablet computer
50	laptop	laptop	laptop	laptop	laptop
51	laptop	laptop	laptop	laptop	laptop
52	Smartphone	Smartphone	Smartphone	Smartphone	laptop

References

Abraheem, A., Bozed, K., & Eltarhouni, W. (2022). Survey of Various Graphical Password Techniques and Their Schemes. *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, pp 105–110. https://doi.org/10.1109/MISTA54861.2022.9837719

Alhojailan, M.I. (2012) Thematic Analysis: A Critical Review of its Process and Evaluation. *West East Journal of Social Sciences*, 1, pp 39-47.

Ann, O.C, & Theng, L.B. (2011). Biometrics based assistive communication tool for children with special needs. In *7th International Conference on Information Technology in Asia*. IEEE, Kuching, Sarawak, Malaysia, pp 1–6.

Amrit, K.J. (2020). Understanding Generation Alpha. Available at: https://osf.io/d2e8g/download [Accessed 27 July 2021]

Anagnostaki, L., Wright, M.J., & Papathanasiou, A. (2013). Secrets and disclosures: How young children handle secrets. *The Journal of genetic psychology* 174(3), pp 316–334.

Anderson, M., & Jiang, J. Teens. (2018) social media & technology 2018. *Pew Research Centre* 31. Available at: https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ [Accessed 29 Jan 2023]

Assal, H., Imran, A., & Chiasson, S. (2018). An Exploration of Graphical Password Authentication for Children. *International Journal of Child-Computer Interaction*, 18, pp 37-46. https://doi.org/10.1016/j.ijcci.2018.06.003

Baron-Cohen, S., Leslie, A. M., & Frith, U. (1985). Does the autistic child have a "theory of mind" ? *Cognition, 21*(1), pp 37–46. https://doi.org/10.1016/0010-0277(85)90022-8

Beck, L.E. (2006). *Child development (7th edition).* Boston, Mass: Pearson Allyn and Bacon.

Bruckman, A., Bandlow, A., Dimond, J,. & Fort, A. (2012). HCI for kids. In Human Computer Interaction Handbook (3rd edition). pp 794-809.

Chartofylaka, L., & Delcroix, A. (2018). StoryPass – Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation. *8th International Toy Research Association World Conference*. Jul 2018, Paris, France.

Choong, Y-Y., Theofanos, M., Renaud, K., & Prior, S. (2019a). Case study: exploring children's password knowledge and practices. In *Proceedings 2019 Workshop on Usable Security (USEC) Internet Society*. San Diego.

Choong, Y-Y., Theofanos, M., Renaud, K., & Prior, S. (2019b). "Passwords protect my stuff" a study of children's password practices, *Journal of Cybersecurity*.*5*(1), pp 1-19.

Coggins, P.E. III. (2013). Implications of what children know about computer passwords. Computers in the Schools, 30(3), pp 282-293.

Cole, J., Walsh, G. & Pease, Z. (2017). Click to enter: comparing graphical and textual passwords for children. In *Proceedings of the 2017 Conference on Interaction Design and Children (IDC '17)*. ACM Press, New York, NY, USA, pp 472-477.

Constantin, A., Korte, J., Good, J., Sim, G., Read, J., Fails, J.A., & Eriksson, E. (2022). A Distributed Participatory Design Research Protocol for Co designing with Children. In *Interaction Design and Children (IDC '22).* Association for Computing Machinery, New York, NY, USA, pp 510–516.

Crain, W.C. (1985). Theories of development (2nd edition). Englewood Cliffs, NJ: Prentice-Hall.

Darbutaite, E., Stefanovic, P. & Ramanauskaite, S. (2023). Machine- Learning -Based Password-Strength-Estimation Approach for Password of Lithuanian Context. *Applied Sciences*, *13* (13), 7811. https://doi.org/10.3390/app13137811

Darroch, A. (2011). Freedom and biometrics in UK schools. *Biometric Technology Today* 2011, 7 (2011), pp 5–7.

Dempsey, J., Cassidy, B., & Sim, G. (2016). Child-Cantered Security. In *30th International BCS Human Computer Interaction Conference (HCI).* http://dx.doi.org/10.14236/ewic/HCI2016.59 .

Dixon, P. (2017). A Failure to “Do No Harm”–India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. *Health and Technology* 7, 4 (2017), pp 539–567.

Ehri, L.C. (1995). Phases of development in learning to read words by sight. *Journal of Research in Reading* 18(2), pp 116–125.

Goswani, U. (2005). Synthetic phonics and learning to read: a cross-language perspective. *Educational Psychology in Practice*, 21(4), pp 273 – 282.

Government of Saudi Arabia, General Authority for Statistics. (2017). Bulletin ICT access and usage by households and individuals survey. page. 42. Available at: https://www.stats.gov.sa/sites/default/files/ict_access_and_usage_by_households_and_individuals_survey_2017en_0.pdf [Accessed 9 April 2019]

Government of Saudi Arabia, General Authority for Statistics. (2018). Bulletin of individuals and households’ ICT access and usage survey. page. 38. Available at: https://www.stats.gov.sa/sites/default/files/bulletin_of_individuals_and_households_ict_2018.pdf [Accessed 9 April 2019]

Hundlani, K., Chiasson, S. & Hamid, L. (2017). No passwords needed: the iterative design of a parent- child authentication mechanism. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '17).* ACM, New York, NY, USA, Article 45, 11 pages.

Hong, K.H., Kang, U.G. & Lee, B.M. (2021). Enhanced Evaluation Model of Security Strength for Passwords Using Integrated Korean and English Password Dictionaries. *Security Communication Network.*

Information Commissioner’s Office. (2020). Age appropriate design: A code of practice for online services. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf. [Accessed 25 November 2022]

Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J. & Aila, T. (2020). Analysing and Improving the Image Quality of StyleGAN. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp 8110–8119. https://arxiv.org/pdf/1912.04958.pdf

Lamichhane, D.R. & Read, J.C. (2017). Investigating children's passwords using a game based survey. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, pp 617-622.

Lamond, M. L., Renaud, K. V., Wood, L. A., & Prior, S. (2022). SOK: young children's cybersecurity knowledge, skills & practice: a systematic literature review. In *EuroUSEC '22: proceedings of the 2022 European Symposium on Usable Security*, pp 14-27. Association for Computing Machinery (ACM). https://doi.org/10.1145/3549015.3554207

Lane, J. (2023). The 10 Most Spoken Languages In The World. Available at: https://www.babbel.com/en/magazine/the-10-most-spoken-languages-in-the-world [Accessed 7 Sep 2023]

Lazar, J., Feng, J.J. & Hochheiser, H. (2010). Research methods in human-computer interaction. Wiley.

Lorenz, B., Kikkas, K. & Osula, K. 2018, "Development of Children's Cyber Security Competencies in Estonia" in Learning and Collaboration Technologies. *Learning and Teaching Springer International Publishing*, Cham, pp 473-482.

Maqsood, S., Biddle, R., Maqsood, S. & Chiasson, S. (2018). An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Child*ren. ACM, New York, NY, USA, pp 539-544.

Markopoulos, P., Read, J.C. and Giannakos, M. (2021). DESIGN OF DIGITAL TECHNOLOGIES FOR CHILDREN. In *HANDBOOK OF HUMAN FACTORS AND ERGONOMICS (eds G. Salvendy and W. Karwowski).* https://doi.org/10.1002/9781119636113.ch49

McCrindle, M., & Fell. A. (2020). Understanding Generation Alpha. McCrindle Research. Available at: https://generationalpha.com/wp-content/uploads/2020/02/Understanding-Generation-Alpha-McCrindle.pdf [Accessed 22 Mar 2023]

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.

Mendori, T., Kubouchi M., Okada M. & Shimizu A. (2002). Password input interface suitable for primary school children. In *Proceedings of the International Conference on Computers in Education (ICCE'02)*. IEEE, pp 765-766.

Merritt, D. D. (2016). Typical speech and language development for school-age children: A checklist for school nurses. Available at: https://ctserc.org/documents/resources/SpeechLanguageDev.pdf [Accessed 28 Feb 2020]

Miller, P. H. (2011). Piaget's theory: Past, present, and future. In U. Goswami (Ed.), *The Wiley-Blackwell handbook of childhood cognitive development*, pp. 649–672. Wiley Blackwell.

NIST Special Publication 800-63B. (2017). Digital identity guidelines. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html [Accessed 20 April 2019]

Ofcom. (2021). Children and parents: Media use and attitudes report 2020/21. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf [Accessed 18 August 2022]

Ofcom. (2022). Children and parents: Media use and attitudes report 2022. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf [Accessed 18 August 2022]

Peyrin, C., Lallier, M., Demonet, J-F., Pernet, C., Baciu, M., Le Bas, J.F, & Valdois, S. (2012). Neural dissociation of phonological and visual attention span disorders in developmental dyslexia: FMRI evidence from two case reports. *Brain and Language* 120(3), pp 381–394.

Prior, S., & Renaud, K. (2020). Age-appropriate password "best practice" ontologies for early educators and parents. In *International Journal of Child-Computer Interaction*, *23*(C). https://doi.org/10.1016/j.ijcci.2020.100169.

Priya, K., Shalmali, M. N, Utkarsha, R. D, Marshini, C., Tamara L. C, & Jessica, V.(2017). 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. In *Proceedings of the ACM on Human-Computer Interaction 1, CSCW* (Dec. 2017), 1–21. DOI:http://dx.doi.org/10.1145/3134699

Ratakonda, D.K., French, T., & Fails, J.A. (2019). My Name Is My Password: Understanding Children's Authentication Practices. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children (IDC'19).* Association for Computing Machinery, New York, NY, USA.

Ratakonda, D. K. (2019). Children's Authentication: Understanding and Usage. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children (IDC'19).* Association for Computing Machinery, New York, NY, USA. ISBN 978-1-4503-6690-8/19/06, https://doi.org/10.1145/3311927.3325354

Ratakonda, D. K., Mehrpouyan, H., & Fails, J. A. (2022). "Pictures are easier to remember than spellings!"'- Designing and evaluating KidsPic — A graphical image-based authentication mechanism. *International Journal of Child-Computer Interaction, 33.* https://doi.org/https://doi.org/10.1016/j.ijcci.2022.100515

Read, J.C. & Cassidy, B. (2012). Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children (IDC '12)*. ACM, New York, NY, USA, pp 200-203.

Read, J.C & Markopoulos, P. (2013). Child–computer interaction, *International Journal of Child-Computer Interaction*, *1*(1), pp 2-6, ISSN 2212-8689, https://doi.org/10.1016/j.ijcci.2012.09.001.

Renaud, K. (2009a). Web Authentication using Mikon Images. *2009 World Congress on Privacy, Security, Trust and the Management of e-Business*, pp 79–88. https://doi.org/10.1109/CONGRESS.2009.10.

Renaud, K. (2009b). Guidelines for designing graphical authentication mechanism interfaces ,*International Journal of Information and Computer Security (IJICS)*, 3(1), pp 60-85, https://doi.org/10.1504/IJICS.2009.026621

Renaud, K., Volkamer, M., Mayer, P., & Grimm, R. (2021). Principles for Designing Authentication Mechanisms for Young Children: Lessons Learned from KidzPass. *AIS Transactions on Human-Computer Interaction*, *13*(4), pp 407-430.

Shannon, C.E. (2001). A mathematical theory of communication. ACM SIGMOBILE Mobile Computing and Communications Review *5*(1), pp 3-55.

Skapyak, M. (2023). Which lessons from child-computer interaction should we bring to the rest of UX? aavailable at: https://uxdesign.cc/which-lessons-from-child-computer-interaction-should-we-bring-to-the-rest-of-ux-796569556c46 [Accessed 07 Oct 2023]

Smorti, A. & Fioretti, C (2019). Beyond the Anomaly: Where Piaget and Bruner Meet. *Integrative Psychological and Behavioral Science*. 53. (4), https://doi.org/10.1007/s12124-019-9477-7

Sowell, E.R, Thompson, P.M, Leonard, C.M, Welcome, S.E, Kan, E., & Toga, A.W. (2004). Longitudinal mapping of cortical thickness and brain growth in normal children. *Journal of Neuroscience*, 24 (38), pp 8223–8231.

Statista Research Department (2022). *Proportion of selected age groups of world population and in regions in 2022*. Statista. Available at: https://www.statista.com/statistics/265759/world-population-by-age-and-region/ [Accessed 21 Mar 2023]

Stewart, M., Campbell, M., Renaud, K., & Prior, S. (2020). Kidzpass: authenticating pre-literate children. In *Proceedings of 2020 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, Iowa USA.

Theofanos, M., Choong, Y-Y., & Murphy, O. (2021). Passwords keep me safe – Understanding what children think about passwords. In *30th USENIX Security Symposium*, pp 19-35.

United Nations International Children's Emergency Fund (unicef). (2017). The state of the world's children 2017: children in a digital world. Available at: https://www.unicef.org/media/48601/file [Accessed 27 August 2022]

Yurtseven, N. & Karadeniz, S. (2020). The Teacher of Generation Alpha Chapter 1. The *Teacher of Generation Alpha*, Berlin, Germany: Peter Lang Verlag.

Ziatdinov, R. & Cilliers, J. (2021). Generation Alpha: Understanding the Next Cohort of University Students, *European Journal of Contemporary Education* 10(3), pp 783-789.