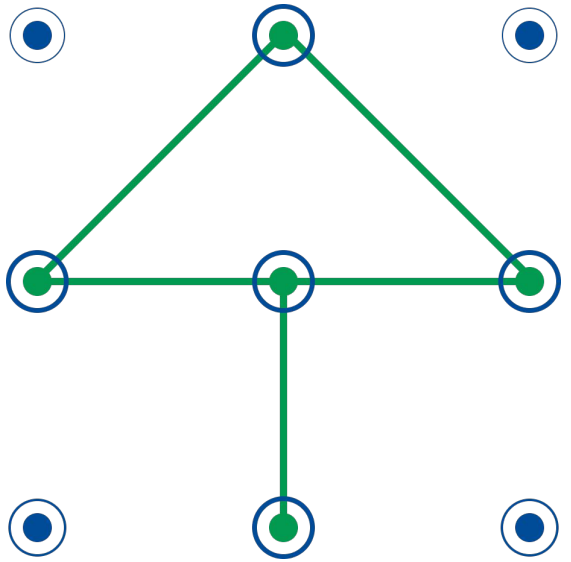
Pattern Power-Up:
Exploring Security and Usability Enhancements in Gesture-Based Passwords



YASH BHARANI

22M2244

INTERACTION DESIGN

M.DES 2nd Year

Project Supervisor

Prof. Anirudh Joshi

12th March 2024

Declaration

I, Yash H. Bharani, hereby declare that this project report, titled "Pattern Power Up" is entirely my own work. All the information, data, and research presented in this report are genuine and have not been submitted in any other form for academic credit or publication. Any external sources used for reference or citation are properly acknowledged in the bibliography section. I take full responsibility for the content, findings, and conclusions presented in this report.

Yash H Bharani
22M2244 | Interaction Design
M Des | IDC School of Design | IIT Bombay (2022-24)

Approval Sheet

Interaction Design Project 2 titled “Pattern Power Up” by Yash H. Bharani (Roll number: 22M2244) is approved for partial fulfillments of the requirements for the degree of “Masters in Design” in Interaction Design at Industrial Design Center, Indian Institute of Technology, Bombay.

Guide: Digital Signature Anirudha N Joshi (i98081) 12-Aug-24 05:52:07 PM

Chairperson:

Internal Examiner:

External Examiner:

Acknowledgement

I would take this opportunity to express my profound gratitude to my advisor, **Professor Anirudha Joshi** for his support and guidance which has been pivotal in this project. His constant feedbacks were always constructive and insightful reflecting his luminary status in the world of interaction design. I am particularly grateful for the casual discussions I had with him which not only alleviated my stress but also provided me a renewed clarity. They played a crucial role in refining the project at every stage. Moreover, the methodological and structural approach my guide imparted has been instrumental in shaping the direction and depth of this research.

I would also like to express my sincere thanks to other faculty members of IDC, especially **Prof. Jayesh Pillai** and **Prof. Swati Pal** for their valuable feedback on this project.

I am deeply thankful to all the participants who generously gave their time and shared their experiences, making this study possible. Their candid feedback and interactions were the cornerstone of this research.

Lastly, a big shoutout to my friends **Sparsh, Anjanesh, Sil & Rutanchi** for their unwavering belief in my capabilities, their encouragement during challenging times, and their celebration of every milestone achieved. Also, thanks to my batchmates at IDC for the collaborative spirits and stimulating discussions that provided a nurturing environment for intellectual growth.

Abstract

This Interaction design and experimental research project aims to explore the modalities offered by Gesture-based Graphical passwords - a prevalent authentication method, especially in mobile devices. The study's primary objective is to evaluate the usability, memorability, and security of enhanced pattern password mechanisms compared to the conventional Android pattern lock.

To achieve this, an application was meticulously designed and developed after numerous iterations and valuable user feedback. This application encompasses four distinct pattern passwords. The first serves as a benchmark, mirroring the traditional Android pattern lock. The subsequent three, termed "Interventions" introduce novel gesture-based interactions

Intervention I: Allows users to revisit a dot multiple times within a single pattern.
Intervention II: Incorporates a hold duration on a dot, registering the length of the hold as part of the authentication.
Intervention III: Grants users the flexibility to craft and submit multiple patterns & taps consecutively.

Employing a between-subjects experimental design, participants are assigned to one of the pattern password along with the benchmark. Their interactions were recorded remotely and analyzed. This research aims to shed light on the potential of gesture-based enhancements in pattern passwords and paves the way for more secure and user-friendly authentication.

Content

Introduction

In today's digital age, the intersection of user experience and security stands at the forefront of technological innovation. As devices become increasingly integral to our daily lives, the methods we employ to secure our personal information must not only be robust, and highly secure but also intuitive and user-friendly. This project, situated within the ambit of the Interaction Design Masters Course, embarks on an exploration of gesture-based pattern graphical passwords, a prevalent authentication paradigm, especially in touchscreen devices.

Introduction

Taxonomy of Passwords

Traditionally, passwords fall into three distinct categories: what you know (knowledge-based), what you have (possession-based), and what you are (biometric-based). Each of these types has its unique advantages and disadvantages in terms of security, usability, and accessibility. Graphical passwords, are a paradigm in authentication mechanisms that leverage visual elements for user authentication that the user remembers.

Departing from traditional alphanumeric approaches, here the user create passwords through graphical input. This innovative method addresses cognitive challenges associated with text-based passwords, offering potential benefits in security and user experience. However, thorough evaluation is imperative to discern their effectiveness against security threats and user preferences.

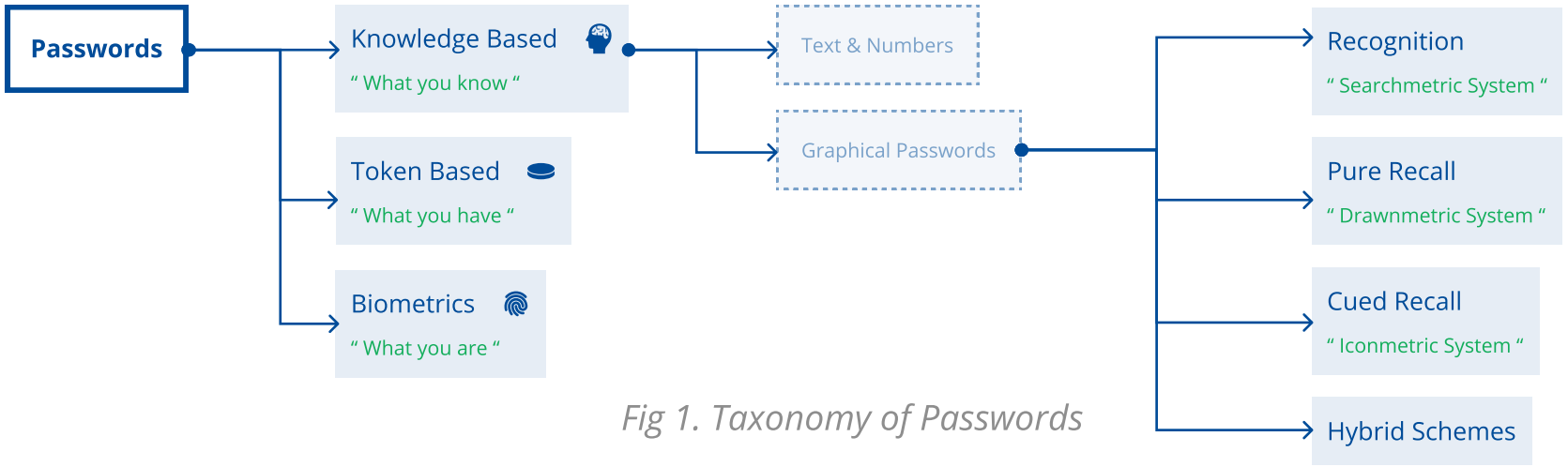


Fig 1. Taxonomy of Passwords

Introduction

Graphical Passwords

Graphical passwords can be grouped into four principal categories [Ref. Fig 2].

1. **Recognition-Based Systems:** Often referred to as Cognometric or Searchmetric systems, these rely on the user's ability to recognize familiar images. Unlike recall-based methods, users are not required to reproduce images from memory. Instead, they identify images they have previously encountered, making the process more about recognition than recall.

2. **Pure Recall-Based Systems:** Also known as Drawnmetric Systems, this category demands users to create the word / symbol or gesture. This method tests the user's memory and ability to accurately reproduce their original input without prompts.

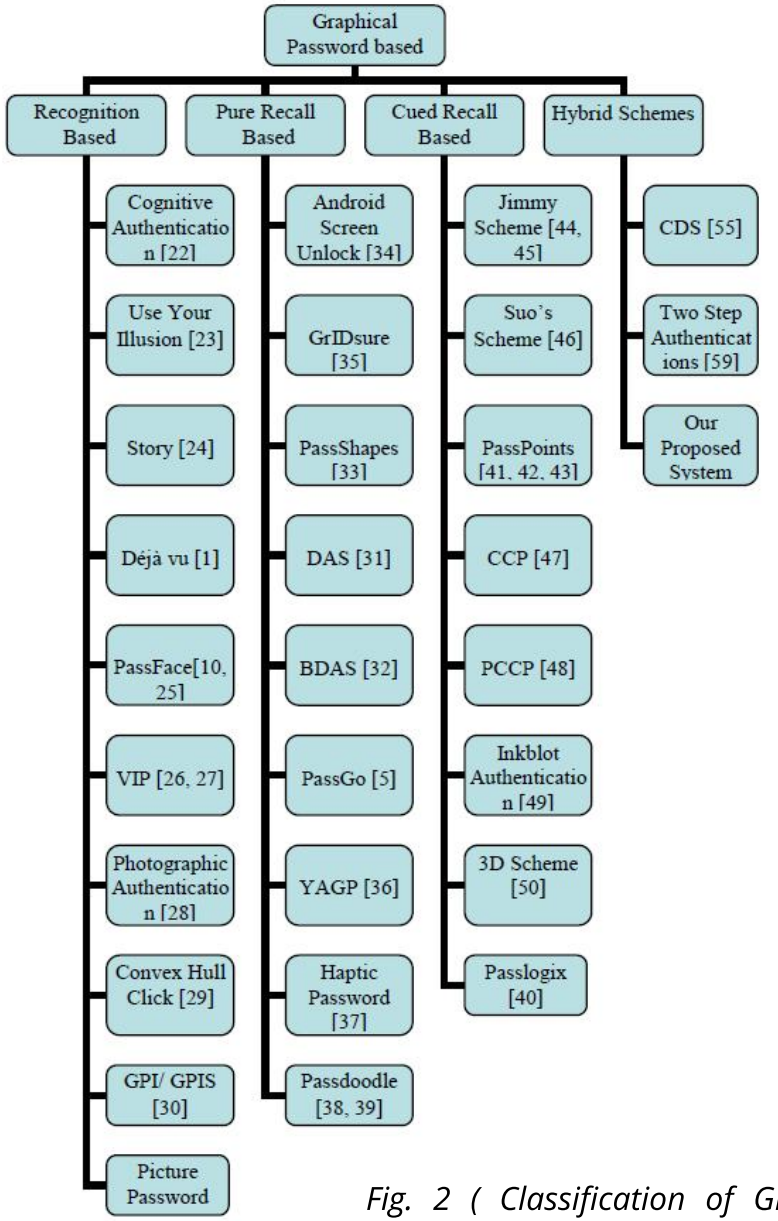
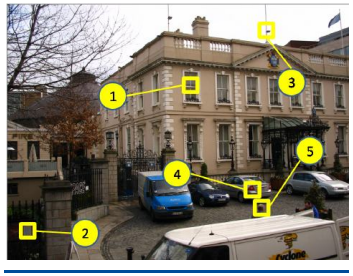


Fig. 2 (Classification of Graphical Password Based Systems)

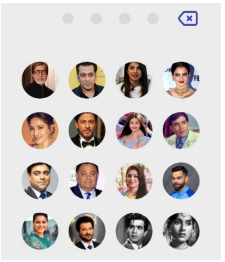
Graphical Passwords

3. **Cued Recall-Based Systems**: Termed Iconmetric Systems, these involve providing users with prompts or cues to aid in recalling their set input. The cues serve as memory triggers, simplifying the password retrieval process by giving hints or partial information.

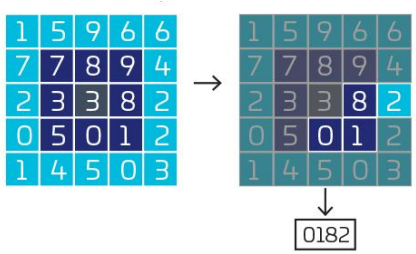
4. **Hybrid Systems**: These are complex schemes that combine elements from two or more of the aforementioned categories. For example, a hybrid system might integrate aspects of recognition and recall-based methods, or blend graphical and textual password elements. The diversity in these systems can offer enhanced security and user convenience by leveraging the strengths of multiple methods [14].



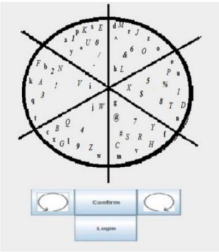
1



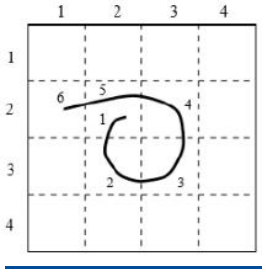
2



3



4



5

Fig. 3.1 Pass Point, 3.2 Pass Faces, 3.3 GrIDsure, 3.4 Spinwheel, 3.5 Draw-a-Secret (DAS) Algorithm

Introduction

Android Pattern Unlock

The Android gesture-based password, commonly known as the "pattern lock," was introduced with Android's version 1.5 "Cupcake" in 2009 as an alternative to traditional PINs and passwords. It leveraged users' ability to remember and recreate patterns on a grid of nine dots, offering a more intuitive and visual method of device authentication.

As for market share, the Android pattern lock is a prevalent security feature. According to an article from The Hindu [1], it is used by around 40% of Android users. Another source from Statista [2] suggests that approximately 32% of global users protect access to their mobile devices using various screen lock methods, including the Android pattern lock.

The research A Study on Usability and Security Features of the Android Pattern Lock Screen [3] highlights its advantages over traditional methods, emphasizing its user-friendliness. The pattern passwords are found to be most preferred by the users, but due to their limited security, their use has been limited to only unlocking phones and apps predominantly. The same conclusions can be drawn from the paper "Draw It As Shown: Behavioral Pattern Lock for Mobile User Authentication" [4] which offers a unique perspective on the Android pattern lock. The authors discuss its standing as a preferred authentication mechanism over traditional PINs or textual passwords, emphasizing its intuitive nature and ease of use.

Introduction

Android Pattern Unlock

Further insights into user behaviour and preferences related to the Android Pattern Lock are provided in "Tell Me Who You Are and I Will Tell You Your Unlock Pattern" [5]. This large-scale user study sheds light on common patterns and tendencies users exhibit when setting their unlock patterns, providing valuable data for enhancing security measures. But overall it is found that the Android pattern locks lack the variations (Entropy) making it even more susceptible to Dictionary Attacks.

The layout and design of the Android unlock pattern also play a crucial role in its usability and security. The research titled "Does the layout of the Android unlock pattern affect the security and usability of the password?" [6] delves into this aspect, investigating the impact of different layouts on user behavior and the overall security of the system. Here they found that that other layouts also work with much greater entropy and security compared to traditional 3x3 matrices. The same results can be found for the PassO interface [7]. The TinPal interface [8], with its visual indicator mechanism, can potentially lead users to create more secure patterns, thereby enhancing the overall security of the pattern lock scheme.

Lastly, striking a balance between usability and security is paramount. The paper "Balancing Usability and Security of Graphical Passwords" [9] discusses this delicate balance, referencing the Android pattern lock and suggesting ways to optimize both aspects for a better user experience.

Challenges of Android Pattern Lock

Based on the possible password space, and the research cited above regarding the usability and the study “A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication” [10], The following chart can be derived (comparative study of the passwords).

Android pattern locks have a balance of usability, memorability, and security, each with its own set of challenges. A study focusing on the usability and security features of the Android pattern lock screen highlights these aspects: [11]

Usability & Memorability: The visual nature of pattern locks enhances memorability. With time, users develop a muscle memory and the retrieval process becomes subconscious. But users tend to prefer usability over security, often choosing simpler patterns for ease of use.

Security Challenges: Despite their popularity, graphical passwords are vulnerable to attacks like shoulder surfing. The simplicity of patterns chosen by many users for convenience can compromise security, as it reduces the overall password space making it prone to dictionary attacks. This underscores the need for more complex patterns to enhance security. Their susceptibility to smudge attacks, where oily residues on the screen can reveal frequently traced patterns, is a notable weakness. Additionally, pattern locks are at risk of brute force attacks due to lack of password space. But these graphical passwords have a very poor communicability, unless a popularly used symbol is used making it less susceptible to phishing attack. To expand the scope of android passwords we need to expand it’s password space and mitigate the other security challenges without much compromise in usability and recall.

Introduction

Challenges of Android Pattern Lock

Table 1: Thematic Comparison of Popular Authentication Schemas

PASSWORD	SPACE	RECALL	USABILITY	SECURITY				USE CASES
				Phishing	Brute Force	Dictionary	Shoulder Surfing	
* * * * * * * * * * * * 12 Character Alphanumeric Password	2.89 x 10 ^ (21)	Least Recall	Worst Usability	◉	◎	◎	◎	Banking Passwords
* * * * * * * * 8 Character Alphanumeric Password	7.22 x 10 ^ (14)	Bad Recall	Bad Usability	◉	◉	◎	◉	Regular passwords for digital accounts
0 0 0 0 0 0 6 Digit Numeric Pin	1 x 10 ^ (6)	Moderate	Average	●	●	●	●	Banking OPT, iOS PIN, safe codes
0 0 0 0 4 Digit Numeric Pin	1 x 10 ^ (4)	Most memorable	Most Usable	●	●	●	◉	ATM Pins, Regular OTP, home lock codes
◉ ◉ ◉ ◉ ◉ ◉ ◉ ◉ ◉ 3x3 Pattern Lock	1.4 x 10 ^ (5)	Good memorability	Good Usability	◎	●	●	●	Android Phone, App Locks

Related Works

The study titled "CharPattern[13]" has made a significant contribution by demonstrating an innovative method of extending the application of Android pattern locks to non-touch-based devices equipped with keyboards, achieving high usability metrics. This advancement has addressed the primary challenge of usability in the adaptation of this password schema as a replacement for traditional alphanumeric passwords. The only hurdle to the adoption of this password schema is its lack of security.

Studies have shown that there is no increment in the security of the pattern passwords with the increase in grid sizes from 3x3 to 4x4. [12]

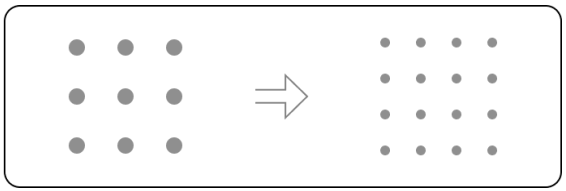


Fig. 4.1 (Increment in the grid size)

In the study “Does the layout of the Android unlock pattern affect the security and usability of the password?”[6], , the researchers changed the layout of the 9 dots from a square to a circle and found that there was a minuscule amount of increment in the password complexities that the users set without much effect on its usability.

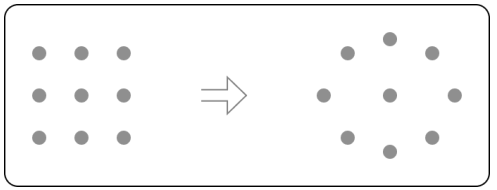


Fig. 4.2 (Change in pattern layout)

There have been many attempts to mitigate these challenges associated with the Android pattern locks. In the paper “Making Graphic-Based Authentication Secure against Smudge Attacks” [14], they tried changing the position of the pattern grid input to address the challenge of smudge attacks (Fig. 5).

Related Works

They found that the tradeoff between usability and security was not sufficient.

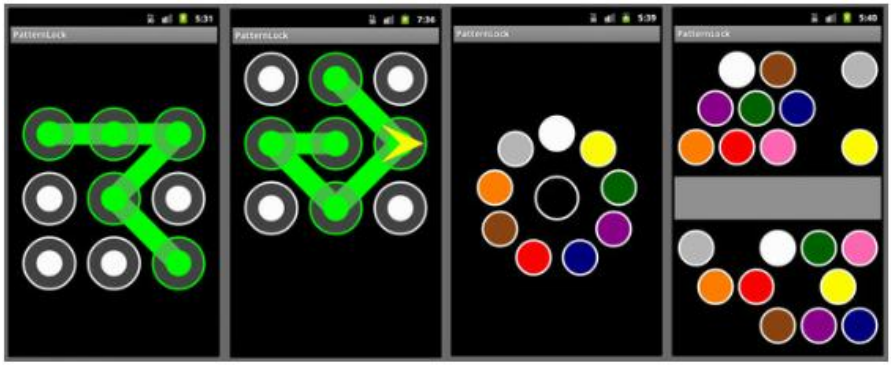


Fig. 5 (The four prototypes of the user study: Android pattern (baseline), pattern 90, marbles and marble gap (from left to right).)

M Pattern [15] on the other hand tried to solve the smudge attack challenge by using 2 different patterns cued by the shown image.

To improve the security and complexity of the patterns that the users set, the SysPal scheme [16] mandates the use of a small number of randomly selected points while selecting a pattern. The result of the study showed that the mandated use of one and two points can help users select significantly more secure patterns without much compromise on recall rates.

Research Objectives

In this study, our objective is to not play with the layout of the pattern, or add visual cues nudging the users to create a more secure password. These interventions have been tested with conclusive results that show that these interventions make a more usable password [12]. However, they do not inherently increase the password space by making use of the affordances that a touch-sensitive display of a mobile phone provides.

The Objective is to explore these affordances and create interactions that ultimately increase the password space of such patterns that will reduce the attack susceptibilities of such gesture-based pattern passwords. Most importantly the Dictionary and the Shoulder Surfing attacks.

Project Justification

Contributions

This exploration and research proposes a novel graphical password-based authentication solution, tailored to be lightweight and cross-platform compatible that adds existing interactions and common gestures to it's defining input method. The solution which is tested amongst participants is rooted in the familiar framework of Android pattern passwords. This solution is designed to be intuitive, ensuring minimal learning curve for users. Key contributions include:

1. **Interaction based Expansion of Password Space**: By integrating more complex pattern options while maintaining user-friendly interfaces, the solution significantly enlarges the password space, addressing a critical limitation of current pattern passwords.
2. **Enhanced Security Against Common Threats**: The interactions are implemented to counter vulnerabilities like shoulder surfing and smudge attacks, bolstering security without compromising usability.
3. **Usability and Memorability**: Despite these enhancements, the system should retains the excellent usability and memorability characteristics of traditional pattern passwords, ensuring a seamless user experience.
4. **Accessibility and Inclusivity**: A notable aspect of this solution is its accessibility. The system should incorporate gesture-based interactions that are easy and practical for a wide range of users, including the elderly and visually challenged, making digital security more inclusive.

Project Justification

FINER Criteria

F

Feasible

The code and logic for pattern authenticator is freely available online for Android Studios along with all the tutorials required for development. It also does not required excess of funds or resources.

I

Interesting

It interests me as I always wanted to learn android studios. I also always hated to remember lengthy passwords.

N

Novel

These interactions have not yet been explored in this context of graphical gesture based passwords. It's design and study can provide valuable insights into potential enhancements for the authentication method.

E

Ethical

Designing a new graphical gesture based password interaction does not seem to curtain any ethical challenges, since such types of passwords are widely accepted in the world.

R

Relevant

About 28.4% of smartphone users use pattern based passwords. In India smartphone users are rising phenomenally and their sensitive information and digital assets are of high importance.

GET IT ON Google Play

Fig. 6 (Landing screens of the test application)

Prototype Design

The journey of creating an application for graphical password authentication started with the identification of interactions that can be used for this research. The design process then began with the design of the visual language of the application with which the users feel familiar. Then we designed the app prototype and took user feedback. It was followed by the development of interactions on Unity, a platform chosen for its cross-platform capabilities. This phase included extensive user testing, leading to iterative refinements in design, interaction, and aesthetics. The development process was punctuated by the introduction of three key interventions aimed at enhancing security and usability. This section provides a comprehensive overview of the challenges, methodologies, and insights encountered during the creation of this prototype.

Prototype Design

App UI

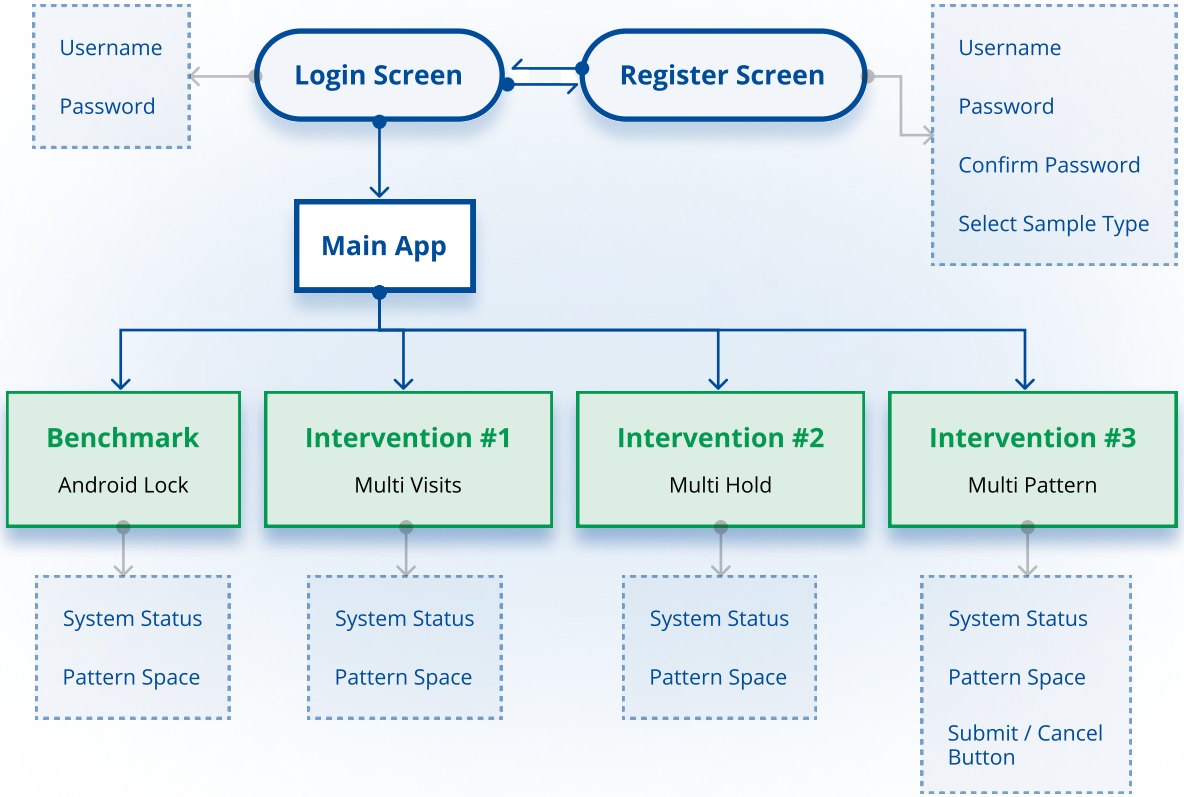
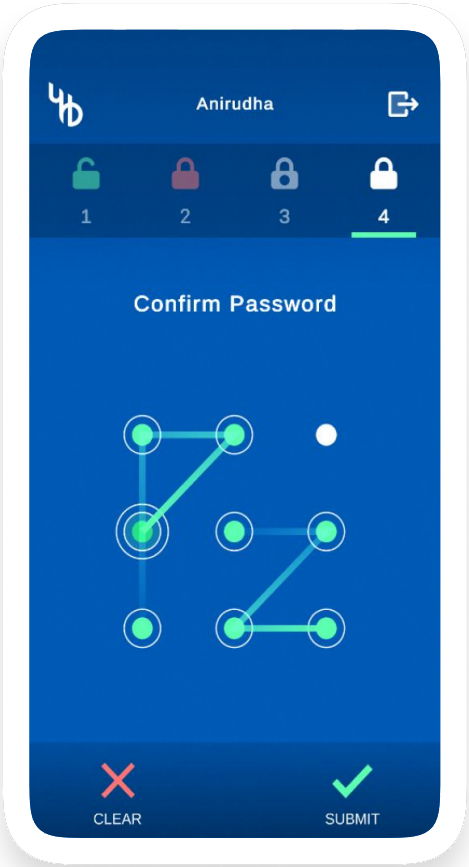


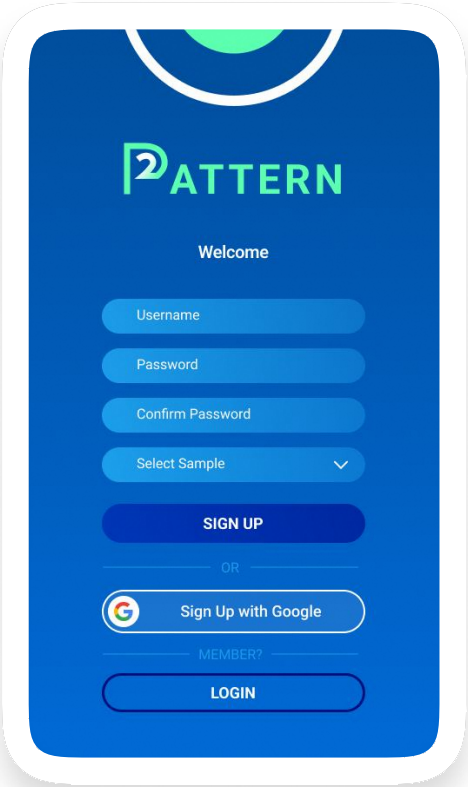
Fig. 7 User Flow

Screen Layout

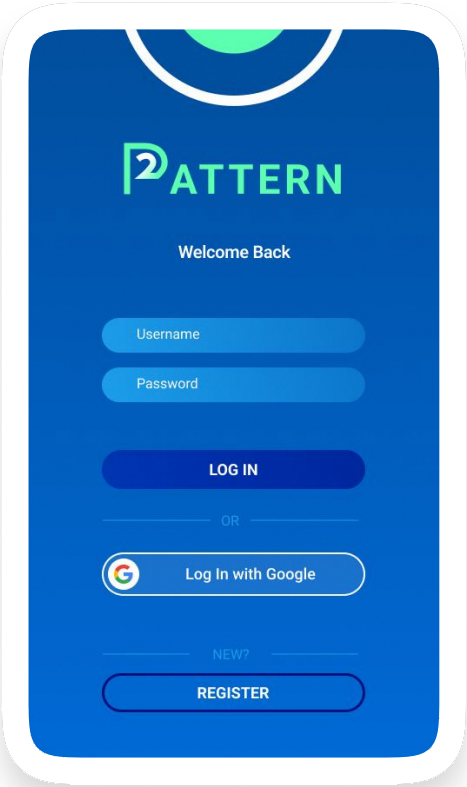


Prototype Design

Screens



Signup Page



Login Page

Colors

#5DFFB1

#5DFFB1

Fonts

Aa **Roboto Bold**

Aa Roboto Light

Prototype Design

Visual Design

Dot States

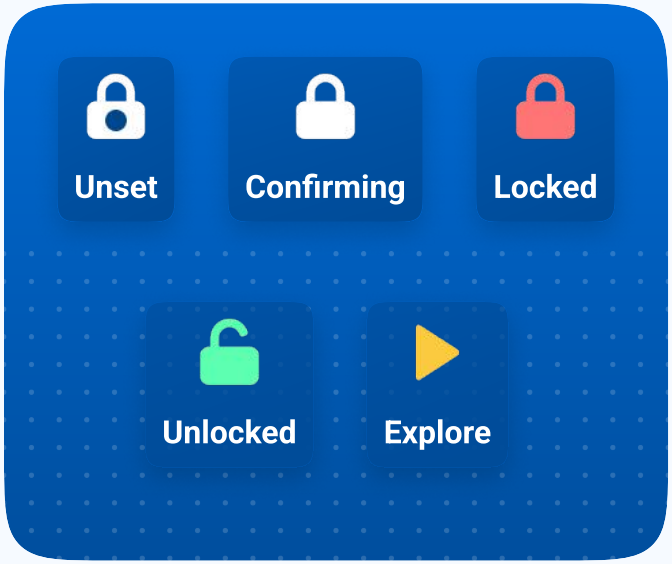
Dots in these new pattern password scheme, don't just have an active/passive state, but they can be configured in 4 distinct states that essentially increases the passwords space hence the security. Visually these states are distinguishable with the adjacent levels.

Line Fading

We had to introduce and distinguish the directionality on the created gesture. Visually we represented this with the fade of the line saturation from behind as the line grows longer.

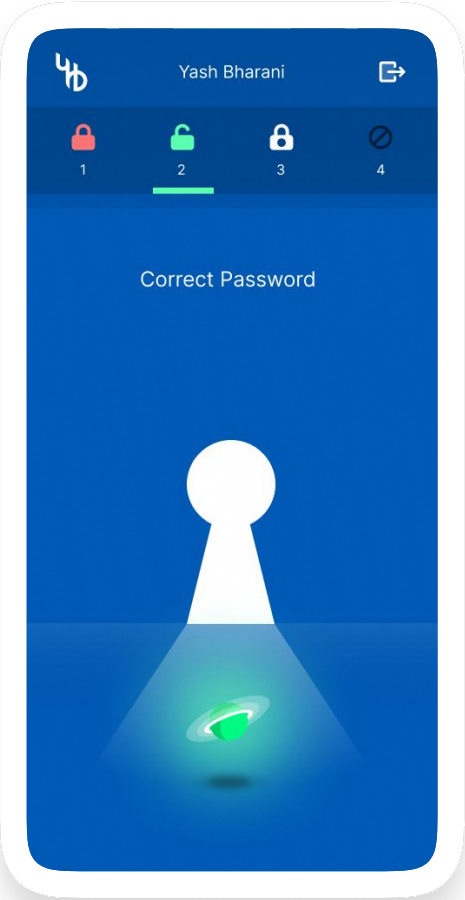
Lock Modes

To introduce a gamification in the process of interacting with the passwords, we have visually defined the modes in which each password type is. Following are the 5 defined modes.



Prototype Design

Backend



Tech Stack Used

Unity

Central development environment and **Engine** for the application. Scripting done in the native **C#** language

Firebase

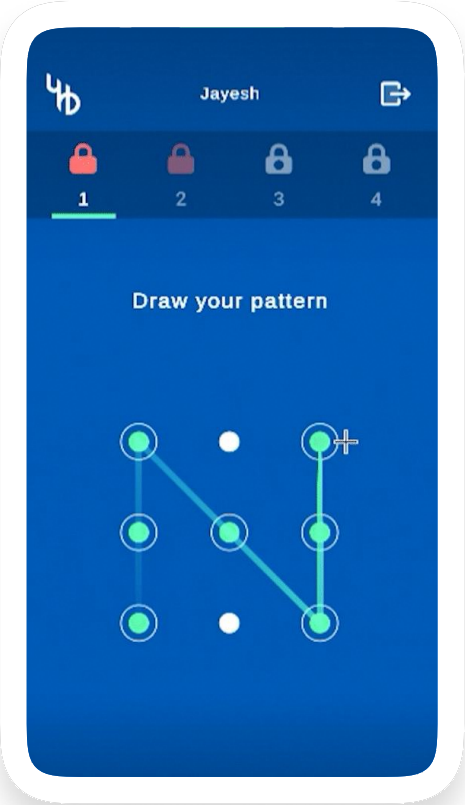
Authentication services and **Realtime Database Creation** of user data and quantitative parameters like error rates, time consumption, etc.

Android

The **primary platform and operating system** for my Unity application. Google Play Store for **distribution, and updates**

Prototype Design

Interventions

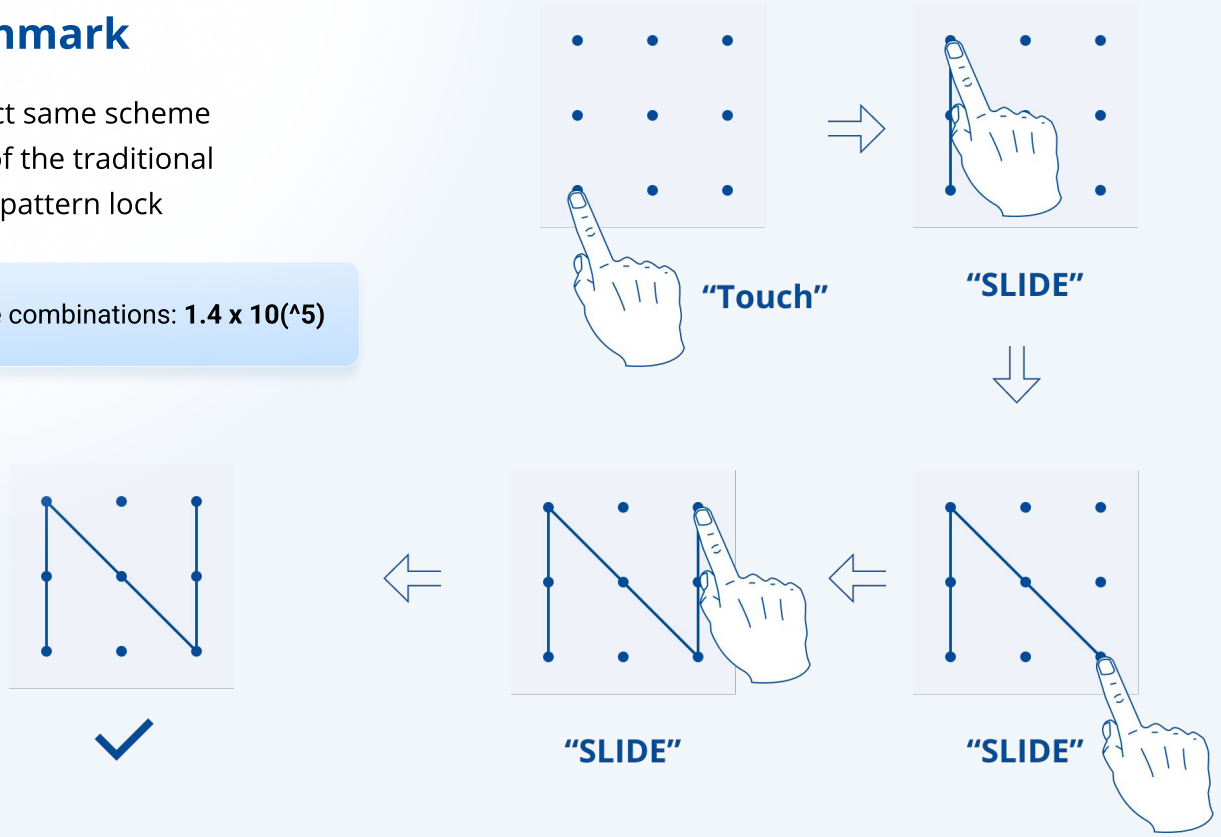


#1

Benchmark

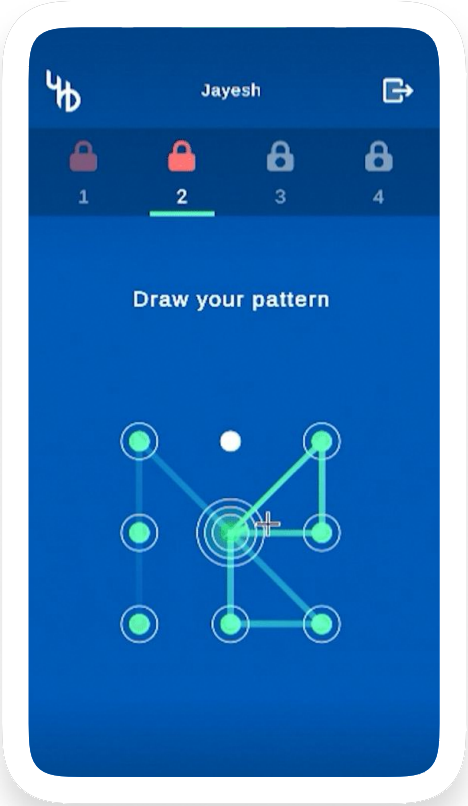
The exact same scheme as that of the traditional android pattern lock

Possible combinations: **1.4 x 10(^5)**



Prototype Design

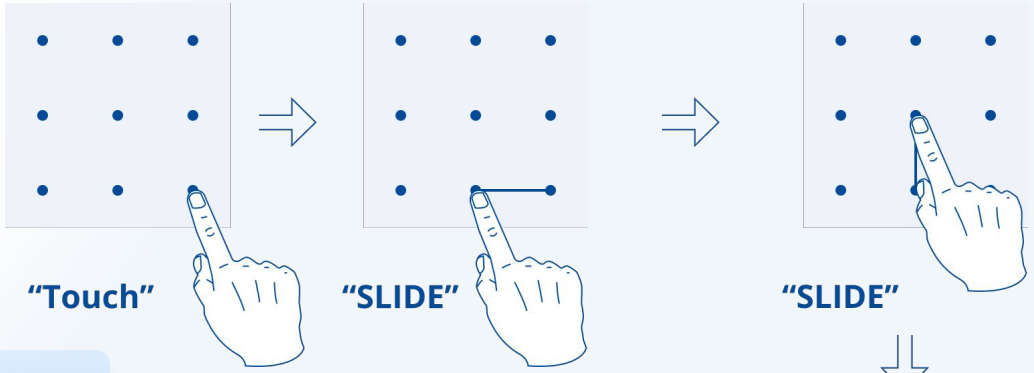
Interventions



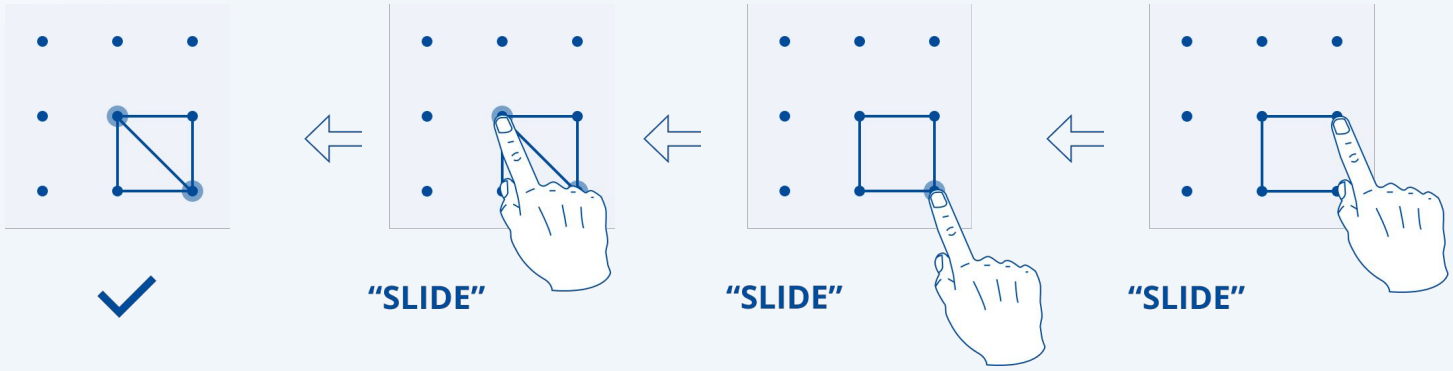
#2

Multi Visit

The users can visit a dot more than once and less than 3 times.

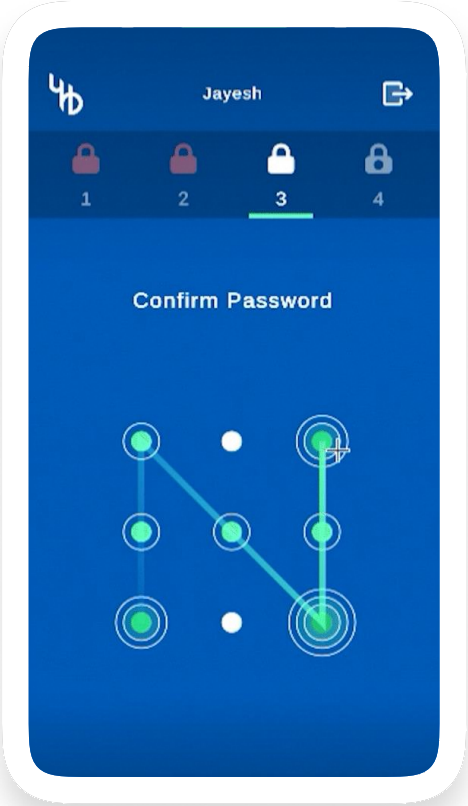


Possible combinations: ~ **2.154 x 10(^7)**



Prototype Design

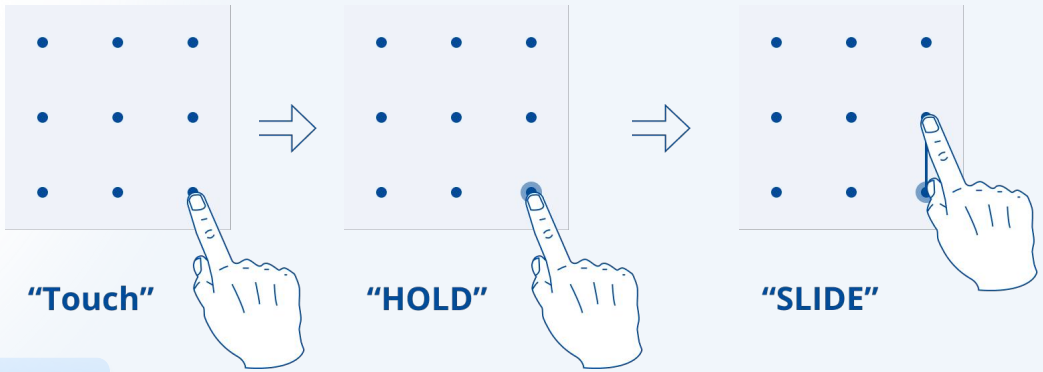
Interventions



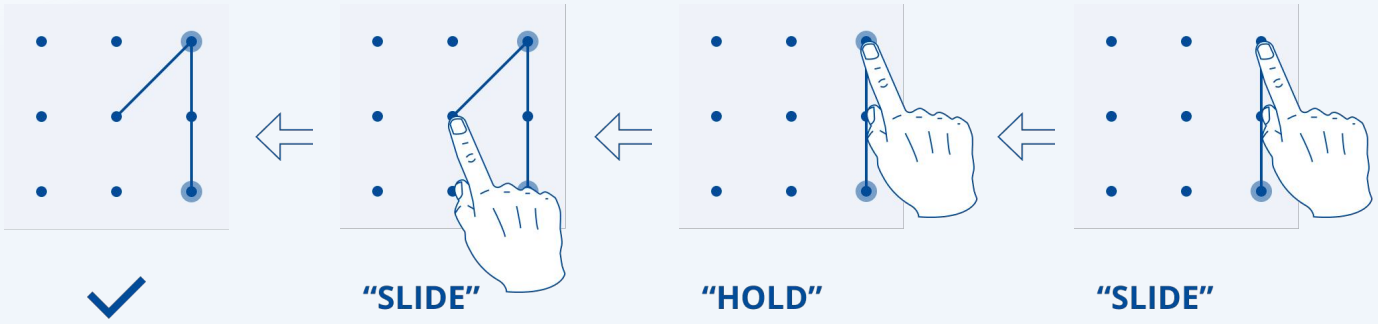
#3

Multi Hold

The users have the option to perform an either short or long hold on to the dot.

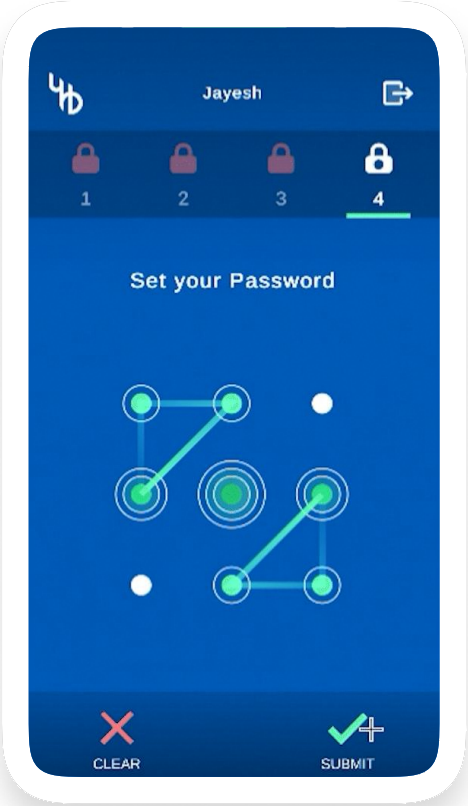


Possible combinations: ~ **6.70 x 10(^10)**



Prototype Design

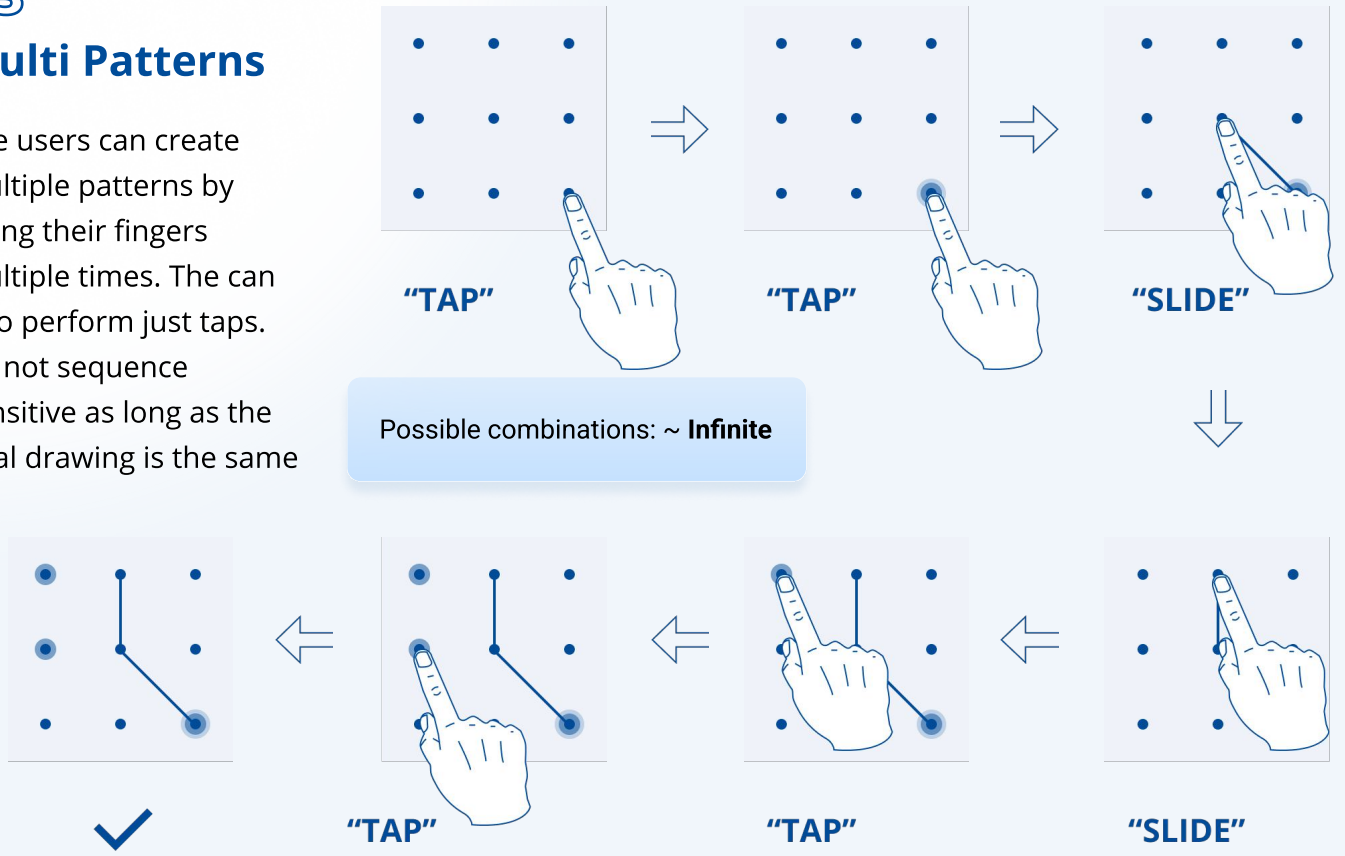
Interventions



#3

Multi Patterns

The users can create multiple patterns by lifting their fingers multiple times. The can also perform just taps. It's not sequence sensitive as long as the final drawing is the same



Research Protocol

A Between Subjects Qualitative and Quantitative Study.

The Aim is to investigate and identify interaction design interventions that can enhance the security of pattern grid gesture-based authenticators. The study will also assess the impact of these interventions on the usability and memorability of the authentication method specifically among the Indian audience.

Scope

1. The design and investigation will be done on a 3x3 dot pattern.
2. Touch-based mobile devices that support Android apps will be used for this project.
3. The assessment will be done on participants across diverse groups of audiences in the IIT Bombay Campus in the allotted time frame of this project.
4. We will do a quantitative as well as a qualitative study on the usability and memorability of different pattern-based password interactions.

Research Questions

RQ#4

Immediate & Delayed Recall

Is there a significant improvement or deterioration in the immediate recalling ability of the suggested pattern interventions, when compared to the existing benchmark?

RQ#5

Error Patterns

Are there specific patterns or commonalities in the errors users make across the different pattern interventions? If so, what are they, and are they significant?

RQ#6

User Preferences

Is there a significant difference in the preference score given by the users between the benchmark and amongst the interventions.

Research Protocol

Variables

Dependent Variables

- **Security:**
  1. **Password Entropy**: The no. of Significantly Different Passwords / Total sample of passwords.

- **Usability:**
  1. **Input Time:** The time taken by the users to input the correct passwords successfully.
  2. **Error Rate:** The no of errors (unsuccessful attempts) made before entering the correct passwords when the user knows the correct password.

- **Memorability:**
  1. **Immediate Recall:** The ability of the users to recall the pattern they set after a short distraction task.
  2. **Delayed Recall:** The ability of the users to recall the pattern they set after each period of day. The longer they retain the password the better.

Control Variables

- The Application
- The Platform (Android)
- User Group
  - They are educated and well-experienced with mobile usage.
  - Belong to the same institute and nationality
- Duration of the recalls (Days for delayed and minutes for Immediate)

Random Variables

- Gender, Age, and Demographics of the participants
- Mobile Phone of the user.

Confounding Variables

- User's experience with the pattern password
- The order in which the user sets and operate their passwords
- Mental state of the user is entering the password.

Research Protocol

Research Design

To investigate the usability, memorability and security parameters of the novel password schemas, we recruited more than 80 people out of which 73 were able to follow through the whole experiment with success. The sample of participants was selected randomly amongst the pool of college students who had android smart phones. All the participants were of similar age group (20-30 yr old) and fairly experienced with using android patterns. Women constituted 27.4% of the total sample.

Each user was given a basic training on how to use the application first. Then they are randomly selected to be a part of one of the 3 test sample groups. Their each session with the app was recorded in the backend.

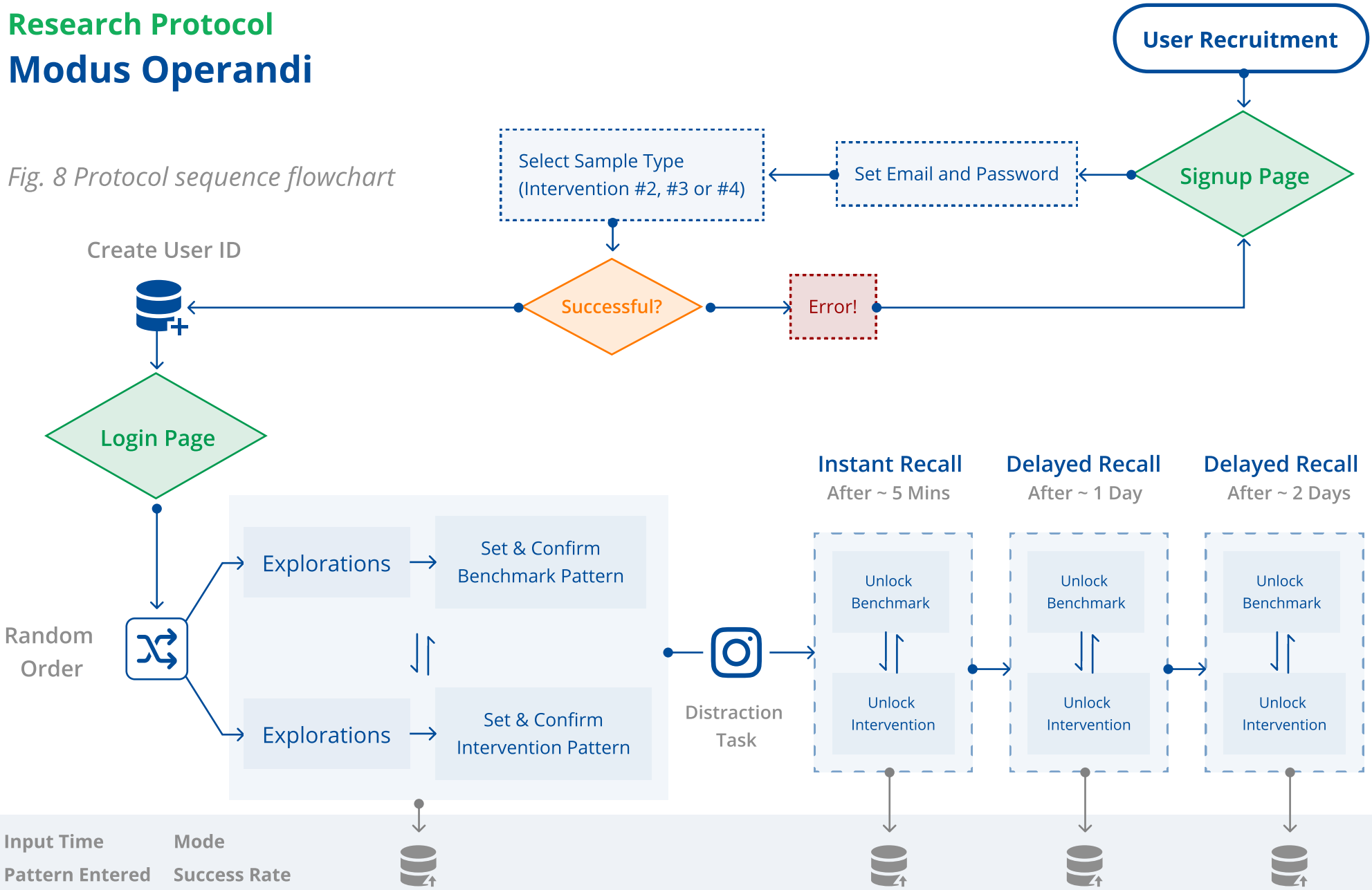
The users interact with the benchmark and one of the interventions in a random order using the tabs. They are told to experiment / play with the patterns first (Exploration stage). Then they are directed to set a pattern as their password in both the schemas which they feel confidant that they can remember for a long durations. They were requested to make use of the available interaction affordances in their sample/intervention type.

After a short distraction task of scrolling the Instagram feed, participants were asked to recall the set password. If they were successful, they were asked to recall again after an interval of 1 day, 2 days and 3 days. The experiment was conducted over a period of 2 weeks with each user engaged for 6 days.

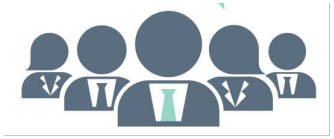
Research Protocol

Modus Operandi

Fig. 8 Protocol sequence flowchart



Data Analysis



73 Participants

25 Multi Visit Sample

24 Multi Hold Sample

24 Multi Pattern Sample

Period:

6 Days

12th to 17th Nov - 2023

It's time to explore the qualitative and the quantitative analysis of user data generated on the three distinct types of pattern passwords developed in this study. The data was screened for outliers and anomalies, which could have been a threat to the validity and reliability of the study. A total of 73 participants were recruited, and assigned to one of the three sample sets. Each sample has 24 participants in the between subject study.

The testing sessions were recorded, and the resulting data were collected and stored on Firebase. Utilizing SQL for data analysis allowed for a detailed and systematic examination of user interactions, response times, error rates, and overall usability metrics for each password type. A separate application was developed on unity to convert the password strings back into the graphical response. This chapter delves into the methodologies employed in the data analysis process, the statistical techniques used, and the insights gleaned from it's comprehensive evaluation.

Data Analysis

Collected Data

Generated form Backend

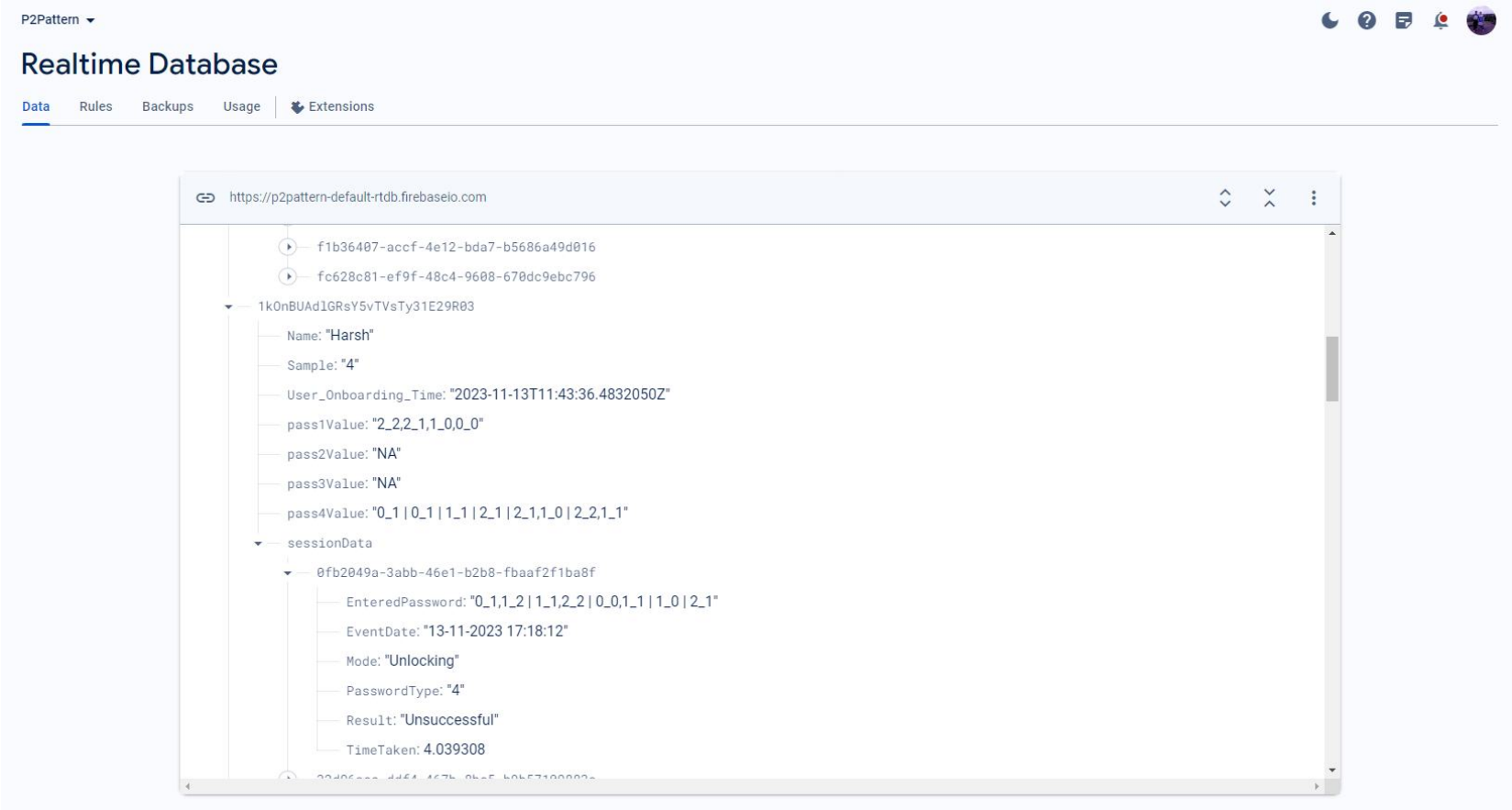


Fig. 9 (Example of the firebase generated database)

Data Analysis

Collected Data

[Link to the excel sheet]

Converted to processable excel sheet

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	eredPassw	EventDate	Mode	asswordTyp	Result	TimeTaken	SessionID	UserID	Name	Sample	Onboarding	pass1Value	pass2Value	pass3Value	pass4Value			
2	0_0,0_2,1_	10-11-202	Unlocking	1	Unsuccess	1.66572	eb2a9438-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
3	0_0,0_1,0_	10-11-202	Unlocking	1	Successful	1.369858	16a74938-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
4	0_0,0_1,0_	10-11-202	Unlocking	1	Successful	1.167997	0b9ae903-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
5		10-11-202	Unlocking	3	Unsuccess	3.786729	5af9ced9-(	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
6		10-11-202	Unlocking	3	Unsuccess	5.188414	2ad2e1c6-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
7		10-11-202	Unlocking	3	Unsuccess	1.975381	1a0ed5ad-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
8	0_0,0_2,1_	10-11-202	Unlocking	1	Unsuccess	1.750271	f406a845-(	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
9	0_0,0_1,0_	10-11-202	Unlocking	1	Unsuccess	3.175768	0d6319fe-(	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
10	0_0,0_0,0_	10-11-202	Unlocking	3	Successful	4.214035	763a4813-	dve2QH2K	Yash	3	2023-11-0	0_0,0_1,0_	NA	0_0,0_0,0_	NA			
11	1_1,1_0,2_	10/11/202	Setting	1	Successful	0.897721	9e784e45-	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
12	1_1,1_0,2_	10/11/202	Confirming	1	Successful	1.099703	83fdc62b-(	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
13		10/11/202	Setting	4	Successful	4.66491	b5e68480-	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
14		10/11/202	Confirming	4	Successful	3.030796	a9a140b2-	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
15		10/11/202	Unlocking	4	Successful	3.663161	ece08ccc-(	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
16	1_1,1_0,2_	10/11/202	Unlocking	1	Successful	0.698731	d8e24b2e-	fjztPA55XV	June	4	2023-11-1	1_1,1_0,2_	NA	NA	| | | | 0_0,1_1 | 1_1 | 1_1,1_0,2_0,2_1,2_2			2_2
17	0_0,1_1,0_	10/11/202	Setting	1	Successful	0.393838	cd08d4ca-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
18	0_0,1_1,0_	10/11/202	Confirming	1	Unsuccess	0.360661	5dc88848-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
19	0_0,1_1,0_	10/11/202	Setting	1	Successful	0.465799	bfbe913a-(	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
20	0_0,1_1,0_	10/11/202	Confirming	1	Successful	0.466416	950b8fb7-(	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
21	0_0,1_1,0_	10/11/202	Unlocking	1	Successful	0.431998	9901f18e-(	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
22	0_0,0_0,1_	10/11/202	Setting	3	Successful	4.899699	08ce91db-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
23	0_0,0_0,1_	10/11/202	Confirming	3	Unsuccess	5.238245	d506513b-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
24	0_0,0_0,1_	10/11/202	Setting	3	Successful	5.030309	ccb17c5c-(	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
25	0_0,0_0,1_	10/11/202	Confirming	3	Unsuccess	5.334701	70b206d3-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
26	0_2,0_1,0_	10/11/202	Setting	3	Successful	3.931477	ee923d91-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
27	0_2,0_1,0_	10/11/202	Confirming	3	Successful	4.000125	d931e485-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
28	0_2,0_1,0_	10/11/202	Unlocking	3	Successful	3.716311	3dc14262-	tzYwhq0o	Sili	3	2023-11-1	0_0,1_1,0_	NA	0_2,0_1,0_	NA			
29	0_0,1_2,2_	10/11/202	Setting	1	Successful	0.704127	35c5560e-	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			
30	0_0,0_1,1_	10/11/202	Confirming	1	Unsuccess	2.830974	8f1a46f5-3	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			
31	0_0,0_1,1_	10/11/202	Confirming	1	Unsuccess	1.332693	be8f6f6a-e	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			
32	0_0,0_1,1_	10/11/202	Confirming	1	Successful	1.265745	d73ce4ba-	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			
33	0_0,0_1,1_	10/11/202	Unlocking	1	Successful	1.098796	6345f481-(	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			
34	0_0,0_1,1_	10/11/202	Unlocking	1	Successful	1.26566	aa8bb8d2-	zpPZuh52	Neha	All	2023-11-1	0_0,0_1,1_	0_0,0_1,0_	0_0,0_0,0_	| | 0_1,1_1,1_2,0_2,0_1,0_0 | 0_2,1_1,2_2,1_1,0_0			

Fig. 10 (Screenshot of the fetched database in google sheets)

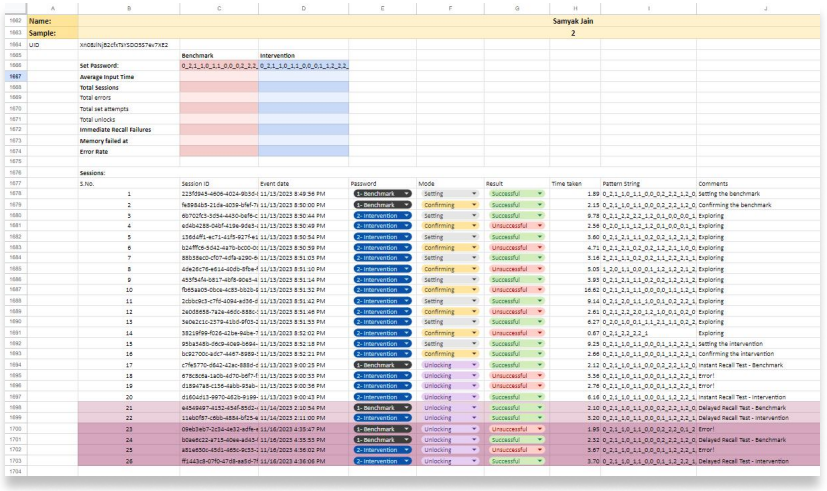
Data Analysis

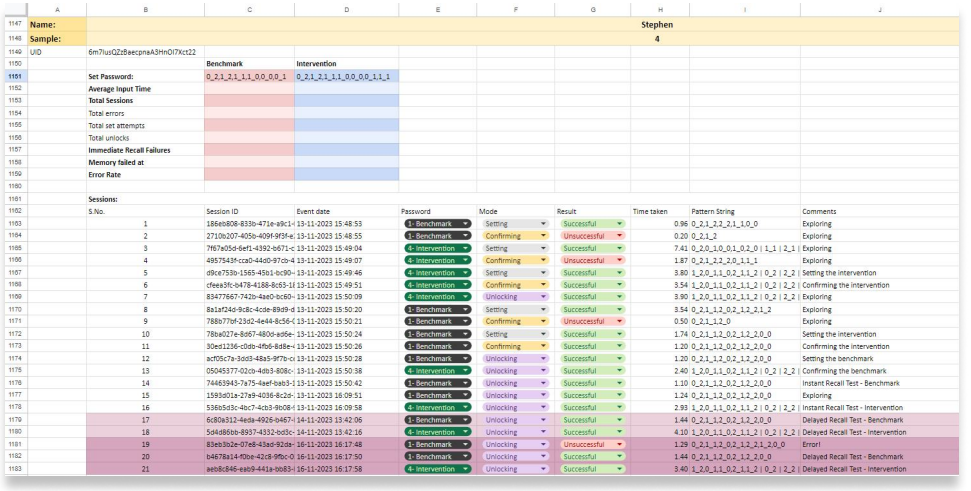
Collected Data

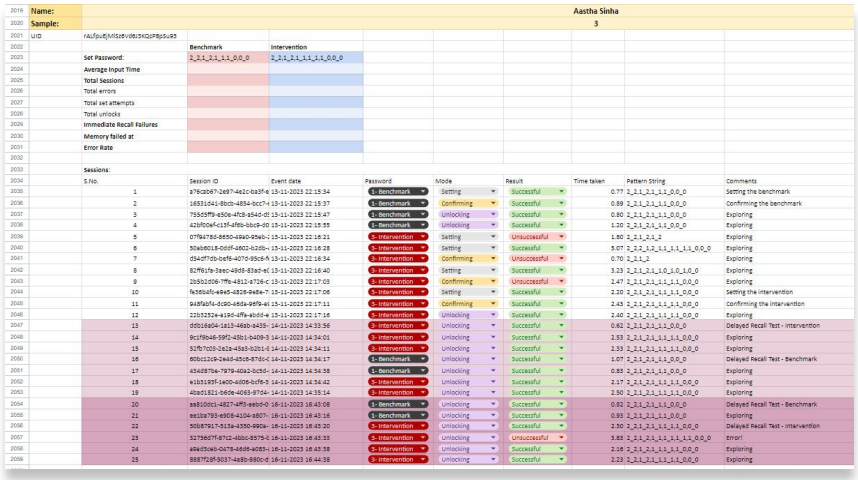
[Link to the excel sheet]

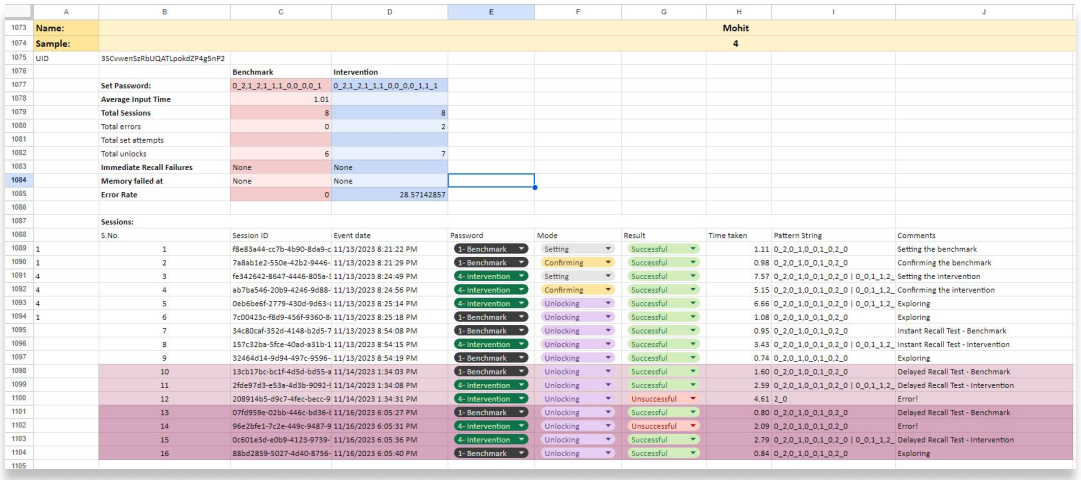
Segregated and tabulated samples

Fig. 11 (Screenshot of the synthesized database created in google sheets)









Data Analysis

Collected Data

[Link to the excel sheet]

Experiment Summary Table

Fig. 12 (Generated database in google sheets)

S.No.	User ID	Sample Type	NAME	GENDER	Onboarded Date / Time	Delayed Recall Test	
						#1 Day 1	#2 Day 3
1	YxA4gUNCMlX	2	Anisha	F	2023-11-11T17:16:52.8389750Z	Done	Done
2	60st19jGG1hRF	4	Suyash	M	2023-11-11T19:15:23.7572020Z	Done	Done
3	9ukY1C0OyDT2	2	Lakha	M	2023-11-11T19:16:29.0194000Z	Forgot both the	-
4	FrH3bkWPchfc	3	Amit Yadav	M	2023-11-11T21:15:25.5804770Z	Forgot the inter	-
5	60st19jGG1hRF	3	Gaurav Shewale	M	2023-11-11T22:53:23.5953210Z	Done	Done
6	mc9Evckzi1YR:	2	SP	M	2023-11-11T22:24:32.2276140Z	Done	Done
7	oHxgmdqhV5h	3	Soni	M	2023-11-11T18:39:45.6083230Z	Done	Done
8	uaULnuPUoKOl	3	Varun	M	2023-11-11T23:07:20.7344180Z	Done	Forgot both b
9	0TjBTajmCjPXs	3	Biswa	M	2023-11-12T06:54:10.4962420Z	Forgot the inter	-
10	35uMygqtvXR8	3	Sangam	M	2023-11-12T07:33:03.9480170Z	Done	Done
11	7DkifwOb9ngH	2	Sangeeth	M	2023-11-12T08:21:00.1315760Z	Done	Done
12	9PxBz32vI9Sh1	4	Ritik	M	2023-11-12T07:56:45.0356490Z	Done	Done
13	He2FV9zIcefTn	4	Mahamuni	M	2023-11-12T06:30:35.1384630Z	Done	Forgot both b
14	LD1D35o80eN:	2	Rutanchi	M	2023-11-12T05:52:25.2806640Z	Done	Done
15	M4880WZZGU	4	Prince	M	2023-11-12T05:38:56.4257430Z	Done	Done

	Set Password
Benchmark	1_2,2_2,1_1,2_1,1_0,0_1,0_0
Intervention	1_2,2_2,1_1,2_1,1_0,0_1,0_0,(
Benchmark	0_2,1_1,1_0,2_0
Intervention	0_2,1_1,1_0,2_0 | 2_1,1_1,0_0
Benchmark	2_2,1_1,0_0,1_0,2_0
Intervention	1_2,1_1,1_0,2_0,2_1,1_2
Benchmark	0_2,0_1,0_0,1_0,2_0
Intervention	0_2,0_2,0_1,0_0,0_0,1_1,2_2,2
Benchmark	0_2,1_2,2_2,1_1,0_0,1_0,2_0
Intervention	0_2,0_2,0_1,0_1,1_1,1_1,1_1,2
Benchmark	2_1,1_1,1_0,2_0
Intervention	1_1,0_2,1_2,2_2,1_1
Benchmark	0_2,0_1,0_0,1_0,2_0
Intervention	0_0,0_0,0_0,1_0,1_0,1_0,2_0,2
Benchmark	0_2,0_1,0_0,1_0
Intervention	0_2,0_1,0_0,0_0,0_0,1_0
Benchmark	0_0,0_1,0_2,1_1,2_2,2_1,2_0
Intervention	0_0,0_0,0_1,0_2,0_2,1_1,1_1,1
Benchmark	2_2,1_2,0_2,0_1,1_1,2_1,2_0,
Intervention	0_2,0_2,0_2,1_1,1_1
Benchmark	2_2,1_1,0_0,1_0,2_0
Intervention	0_0,1_1,0_0,1_0
Benchmark	0_2,0_1,0_0,1_0,2_0
Intervention	0_1,0_0 | 0_2,1_1 | 2_1,2_0 | 2
Benchmark	0_2,0_1,0_0,1_0,2_0
Intervention	0_2,0_1,0_0,1_0,2_0 | 1_1 | 1_
Benchmark	0_2,0_1,1_2,0_0,1_1,2_2,1_0,2
Intervention	1_1,1_2,0_1,1_0,2_1,1_1,1_2,(
Benchmark	0_2,0_1,0_0,1_0,2_0
Intervention	0_2,0_1,0_0,1_0,2_1,1_1,0,2

Data Analysis

Recall Test

Link to the excel sheet

Immediate Recall	All 73 Users Passed the Immediate Recall Test						
Delayed Recall #1	**Multi Visit**		**Multi Hold**		**Multi Pattern**		**Users Passed**
	Forgot the Benchmark	0	Forgot the Benchmark	0	Forgot the Benchmark	1	**67**/73
	Forgot the Intervention	0	Forgot the Intervention	3	Forgot the Intervention	0	
	Forgot Both	1	Forgot Both	0	Forgot Both	1	
Delayed Recall #2	**Multi Visit**		**Multi Hold**		**Multi Pattern**		**Users Passed**
	Forgot the Benchmark	0	Forgot the Benchmark	0	Forgot the Benchmark	0	**62**/67
	Forgot the Intervention	0	Forgot the Intervention	2	Forgot the Intervention	1	
	Forgot Both	0	Forgot Both	1	Forgot Both	1	

Summary	**Benchmark Failure rate:**	**Multi Visit Failure Rate**	**Multi Hold Failure Rate**	**Multi Pattern Failure Rate**
	5/73 = **6.8%**	1/25 = **4%**	6/24 = **25%**	3/24 = **12.5%**

Table 2 : Results summary of the recall test

Data Analysis

Input Time

For the multi visit sample:

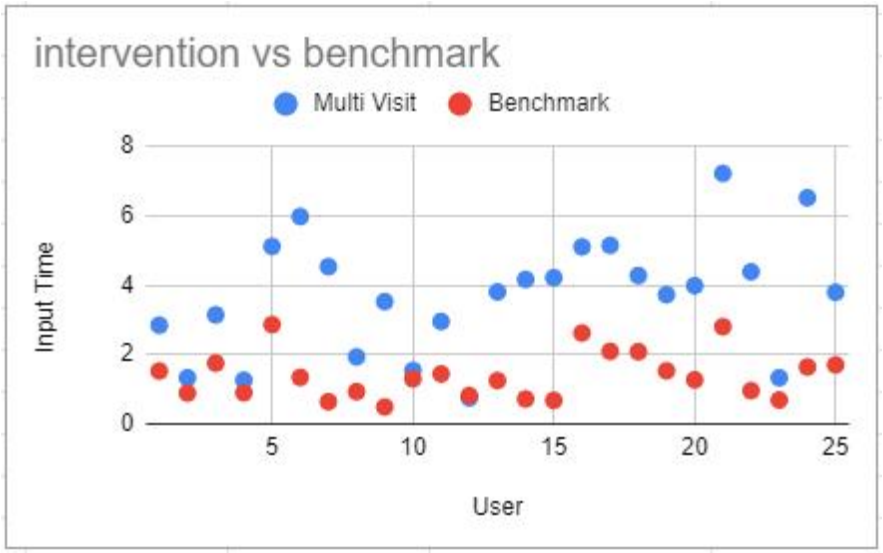


Fig. 13 (Scatter Plot of input times - benchmark and Multi Visit across users)

For the sample size of 25, the Multi Visit pattern schema takes ~2 sec longer on average and is found significantly longer than the benchmark by the student's paired t-test.

benchmark	intervention			Dataset 1	Dataset 2
1.523726	2.842147	1	N	25	
0.89	1.33	2	SD of the sample s	0.7	
1.75	3.14	3	Observed mean	1.4	
0.9	1.26	4			
2.9	5.1	5	Paired t test	-5.213	
1.3	6.0	6	Degrees of freedom	24	
0.6	4.5	7	P value (two tailed)	0.00000014524(	
0.9	1.9	8			
0.5	3.5	9			
1.3	1.54	10			
1.44	2.95	11			
0.82	0.75	12			
1.25	3.8	13			
0.72	4.16	14			
0.68	4.21	15			
2.62	3.10	16			
2.09	3.14	17			
2.08	3.27	18			
1.53	3.72	19			
1.27	3.98	20			
2.8	7.21	21			
0.96	4.38	22			
0.69	1.33	23			
1.64	4.51	24			
1.7	3.79	25			

Fig. 14 (Data of input times - benchmark, multi visit and the t-test results)

Data Analysis

Input Time

For the multi hold sample:

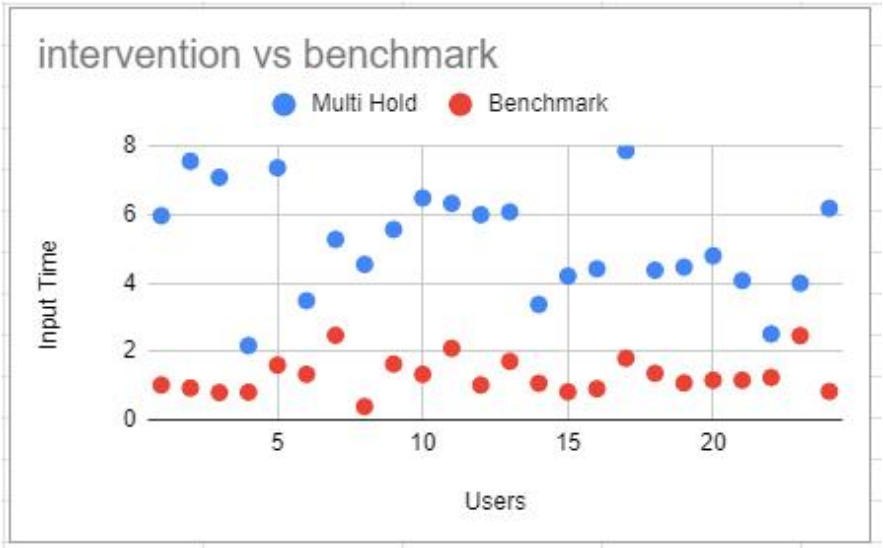


Fig. 15 (Scatter Plot of input times - Benchmark and Multi Hold across users)

For the sample size of 24, the Multi Hold pattern schema takes ~3.9 sec longer on average and is found significantly longer than the benchmark by the student's paired t-test.

benchmark	intervention			Dataset 1	Dataset 2
1.02	5.96	1	N	24	24
0.93	7.55	2	SD of the sampl	0.5	1.6
0.799039125	7.079055333	3	Observed mean	1.3	5.2
0.81	2.17	4			
1.6	7.4	5	Paired t test	-8.214	
1.3	3.5	6	Degrees of freec	23	
2.5	5.3	7	P value (two taile	0	
0.4	4.5	8			
1.6	5.6	9			
1.33	6.48	10			
2.09	6.32	11			
1.02	5.99	12			
1.71	6.07	13			
1.07	3.37	14			
0.82	4.2	15			
0.91	4.41	16			
1.8	7.86	17			
1.36	4.37	18			
1.08	4.46	19			
1.16	4.79	20			
1.16	4.07	21			
1.23822	2.509	22			
2.46	3.99	23			
0.83	6.18	24			

Fig. 16 (Data of input times - benchmark, multi hold and the t-test results)

Data Analysis

Input Time

For the multi pattern sample:

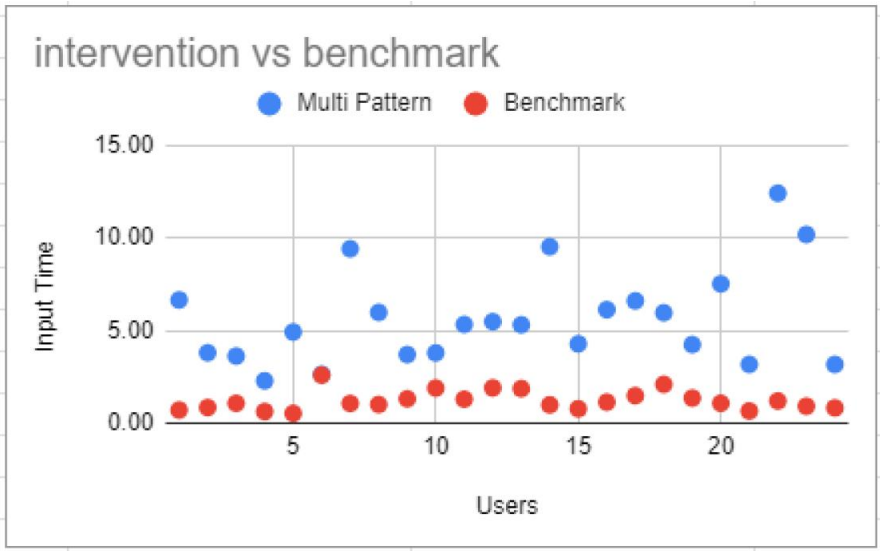


Fig. 17 (Scatter Plot of input times - Benchmark and Multi Pattern across users)

benchmark	intervention			Dataset 1	Dataset 2
0.71	6.66	1	N	24	24
0.85	3.81	2	SD of the sample s	0.5	2.6
1.08	3.63	3	Observed mean	1.2	5.7
0.63	2.29	4			
0.5	4.9	5	Paired t test	-6.717	
2.60	2.6	6	Degrees of freedom	23	
1.1	9.4	7	P value (two tailed)	0.0000003262269713	
1.0	6.0	8			
1.3	3.7	9			
1.9	3.8	10			
1.3	5.34	11			
1.91	5.49	12			
1.87	5.32	13			
0.99	9.54	14			
0.78	4.29	15			
1.14	6.14	16			
1.49	6.61	17			
2.1	5.97	18			
1.36	4.25	19			
1.08	7.53	20			
0.66	3.18	21			
1.2	12.43	22			
0.92	10.2	23			
0.83	3.18	24			

Fig. 18 (Data of input times - benchmark and multi pattern and the t-test results)

For the sample size of 24, the Multi Pattern password schema takes ~4.5 sec longer on average and is found significantly longer than the benchmark by the student's paired t-test.

Data Analysis

Error Rates

For the multi visit sample:

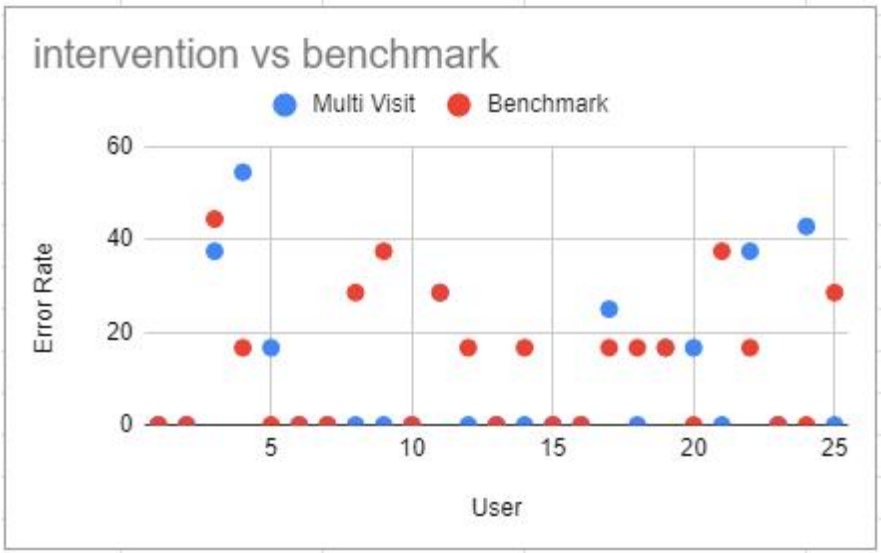


Fig. 19 (Scatter Plot of Error rates - benchmark and Multi Visit across users)

For the sample size of 25, No significant difference was found between the Multi Visit password schema by the student's paired t-test (p-value: 0.650). But the benchmark showed more error rates.

benchmark	intervention			Dataset 1	Dataset 2
0	0	1	N	25	25
0	0	2	SD of the sample s	14.5	16.9
44.44444444	37.5	3	Observed mean	12.9	11.0
16.66666667	54.54545455	4			
0.0	16.7	5	Paired t test	0.597	
0.0	0.0	6	Degrees of freedom	24	
0.0	0.0	7	P value (two tailed)	0.6502541635	
28.6	0.0	8			
37.5	0.0	9			
0	0	10			
28.57142857	28.57142857	11			
16.66666667	0	12			
0	0	13			
16.66666667	0	14			
0	0	15			
0.00	0.00	16			
16.66666667	25	17			
16.66666667	0	18			
16.66666667	16.66666667	19			
0	16.66666667	20			
37.5	0	21			
16.66666667	37.5	22			
0	0	23			
0	42.85714286	24			
28.57142857	0	25			

Fig. 20 (Data of Error rates - benchmark, multi visit and the t-test results)

Data Analysis

Error Rates

For the multi hold sample:

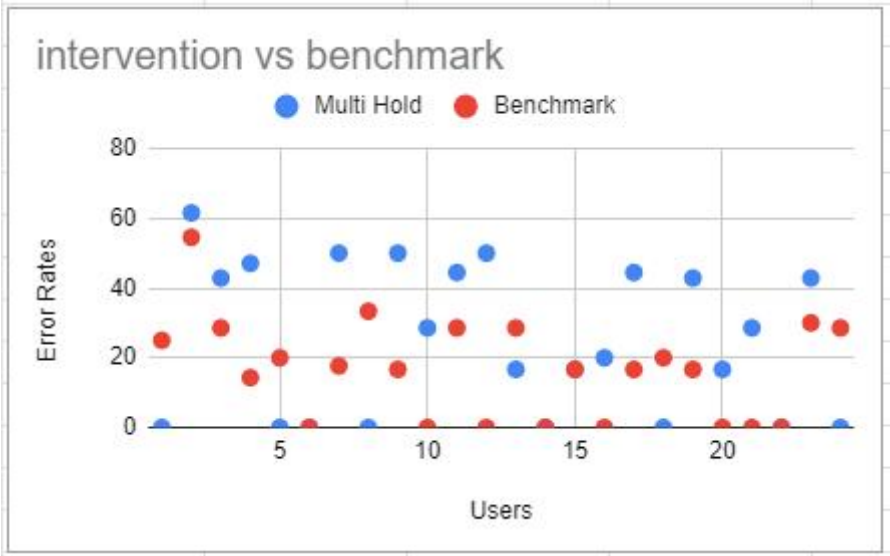


Fig. 21 (Scatter Plot of Error rates - benchmark and Multi Hold across users)

For the sample size of 24, Almost significant difference of 8.6% was found between the Multi Visit password schema by the student's paired t-test (p-value: 0.075). We can conclusively state that this schema entails more error than the benchmark.

benchmark	intervention			Dataset 1	Dataset 2
25	0	1	N	24	24
54.54545455	61.53846154	2	SD of the sampl	14.4	21.5
28.57142857	42.85714286	3	Observed mean	16.5	25.1
14.28571429	47.05882353	4			
20.0	0.0	5	Paired t test	-1.878	
0.0	0.0	6	Degrees of freec	23	
17.6	50.0	7	P value (two taile	0.07516989964	
33.3	0.0	8			
16.7	50.0	9			
0	28.57142857	10			
28.57142857	44.44444444	11			
0	50	12			
28.57142857	16.66666667	13			
0	0	14			
16.66666667	16.66666667	15			
0.00	20.00	16			
16.66666667	44.44444444	17			
20	0	18			
16.66666667	42.85714286	19			
0	16.66666667	20			
0	28.57142857	21			
0	0	22			
30	42.85714286	23			
28.57142857	0.00	24			

Fig. 22 (Data of Error rates - benchmark, multi hold and the t-test results)

Data Analysis

Error Rates

For the multi pattern sample:

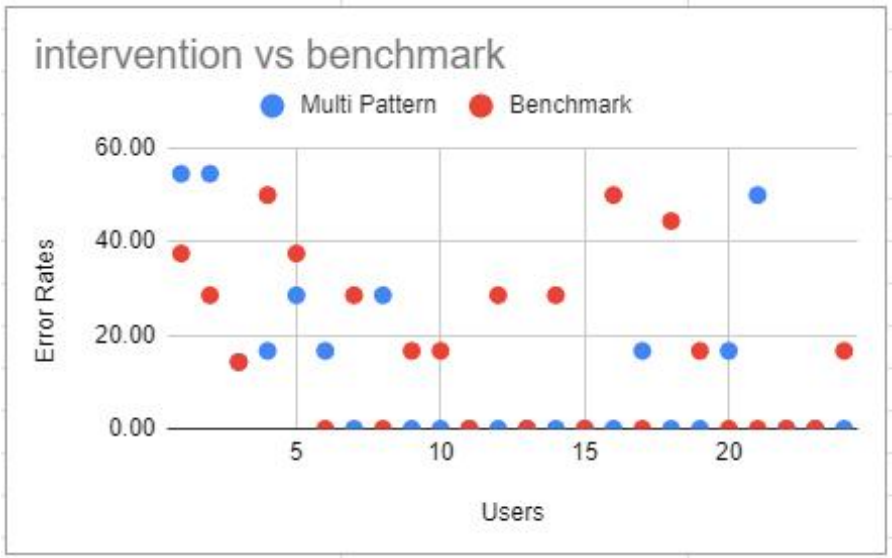


Fig. 23 (Scatter Plot of Error rates - benchmark and Multi Pattern across users)

benchmark	intervention			Dataset 1	Dataset 2
37.50	54.55	1	N	24	24
28.57142857	54.54545455	2	SD of the sample s	17.7	18.3
14.29	14.28571429	3	Observed mean	17.3	12.4
50	16.66666667	4			
37.5	28.6	5	Paired t test	1.433	
0.00	16.7	6	Degrees of freedom	23	
28.6	0.0	7	P value (two tailed)	0.3371137402	
0.0	28.6	8			
16.7	0.0	9			
16.66666667	0	10			
0	0	11			
28.57142857	0	12			
0	0	13			
28.57	0	14			
0	0	15			
50.00	0.00	16			
0	16.67	17			
44.44444444	0	18			
16.66666667	0	19			
0	16.66666667	20			
0	50	21			
0	0	22			
0	0	23			
16.66666667	0.00	24			

Fig. 24 (Data of Error rates - benchmark, multi pattern and the t-test results)

For the sample size of 24, No significant difference was found between the Multi pattern password schema by the student's paired t-test (p-value: 0.337). Here also the benchmark showed slightly more error rates than the intervention.

Data Analysis

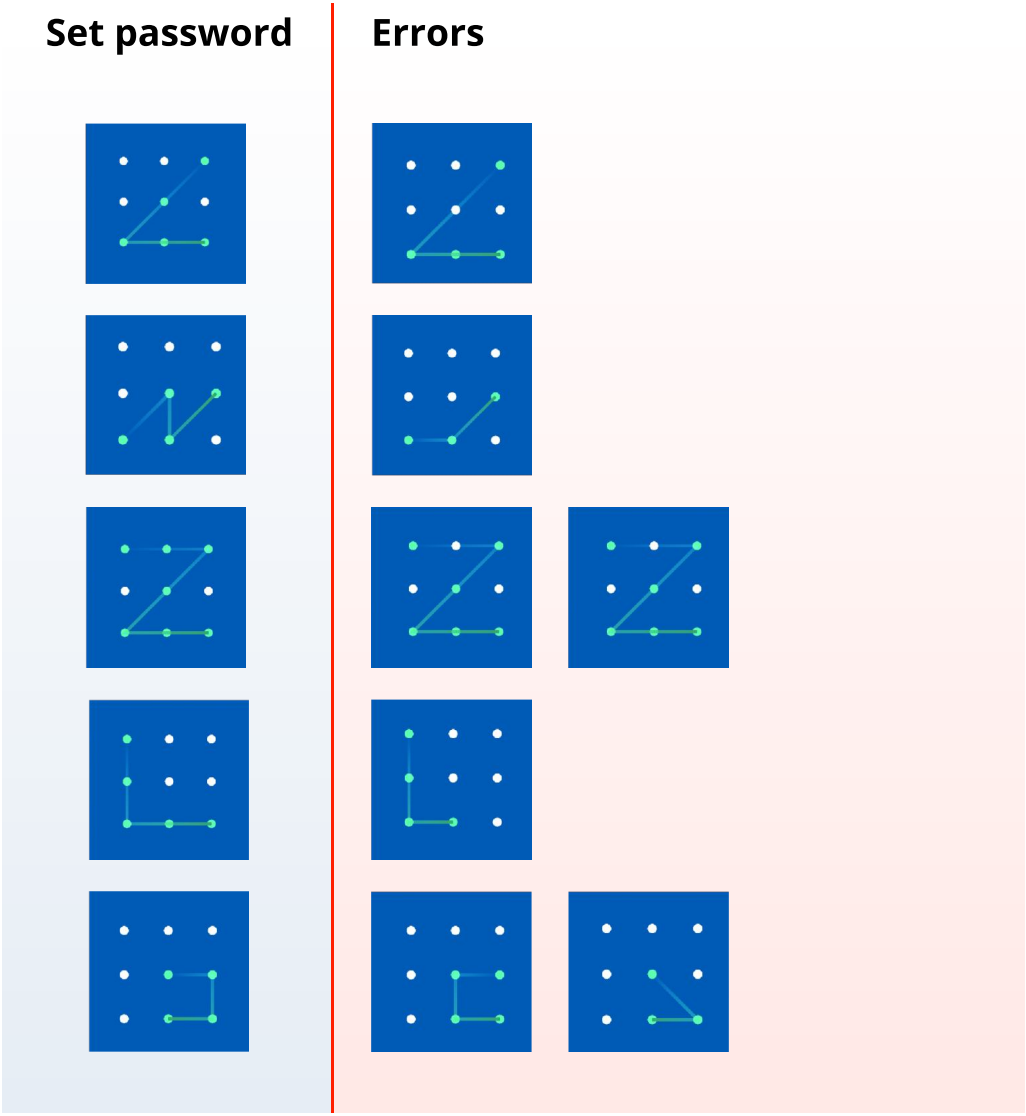
Error Analysis

When we saw the errors that the users are making in the four designed password schemas, we could clearly identify some patterns and the common usability challenges that were present in them.

The Benchmark:

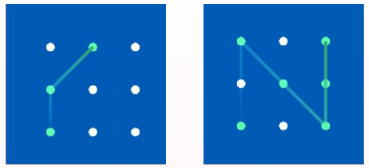
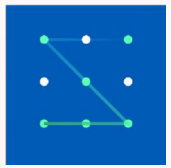
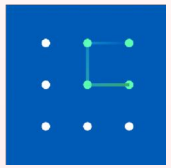
One of the most significant trend that was observed was that the users were very quick and confidant while inputting their password patterns compared to the other interventions where they were much more conscious regarding their actions . Since its a fairly quick process of inputting, users also didn't mind the errors that much. The result was that the most of the errors that were inputted constituted of missing one or 2 dots in haste.

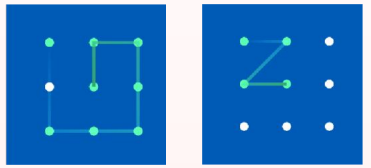
Table 3 : Common trends in errors - benchmark



Error Analysis

Table 3 : Common trends in errors - benchmark

Set password	Errors
	
	
	
	
	

Set password	Errors
	
	
	
	
	

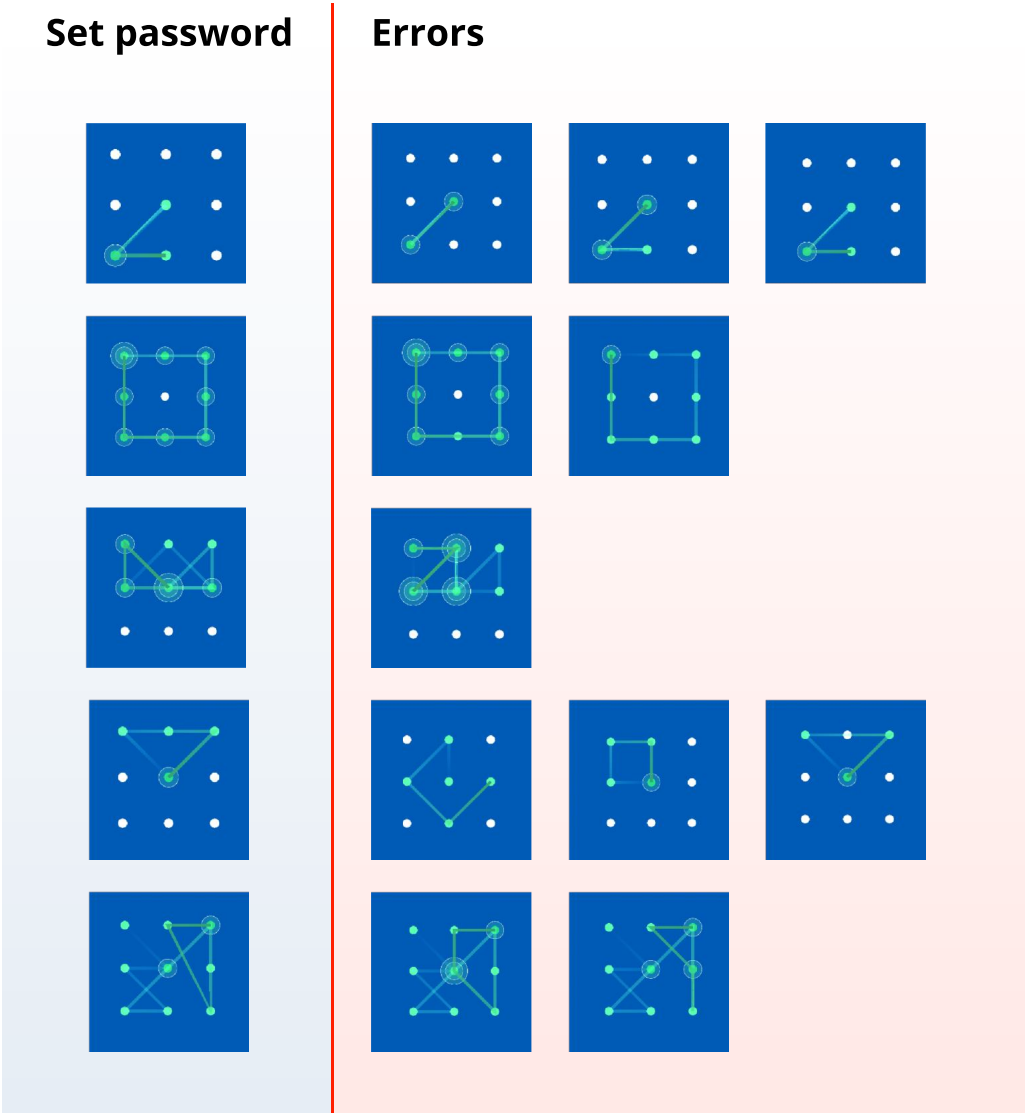
Error Analysis

Table 4 : Common trends in errors - multi visit

The Multi Visit Password Schema:

The errors in this schema followed a similar trend as that of the benchmark, as they (users) hastily entered the pattern without hesitancy.

Participants who did repeated strokes tend to forget the number of times they repeated the swipe, and tried multiple times until they got the correct results. The gradient in the stroke showed to help them remember the complex password better.

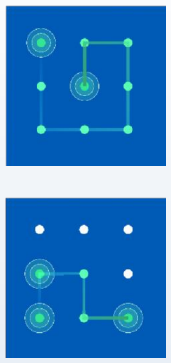
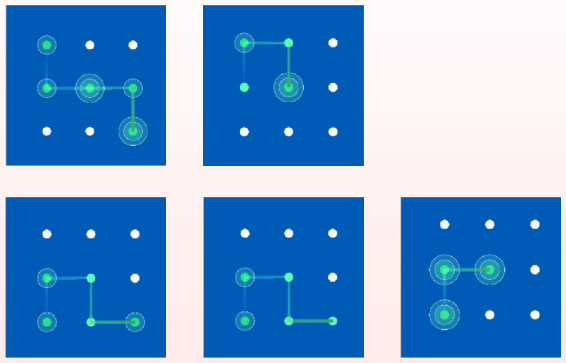


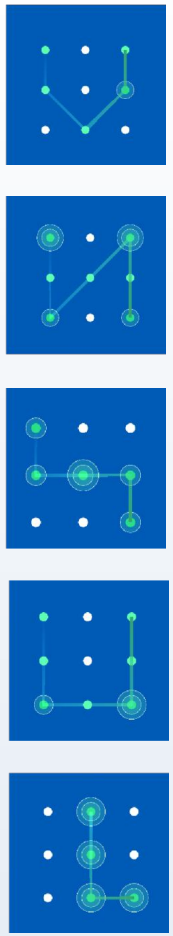
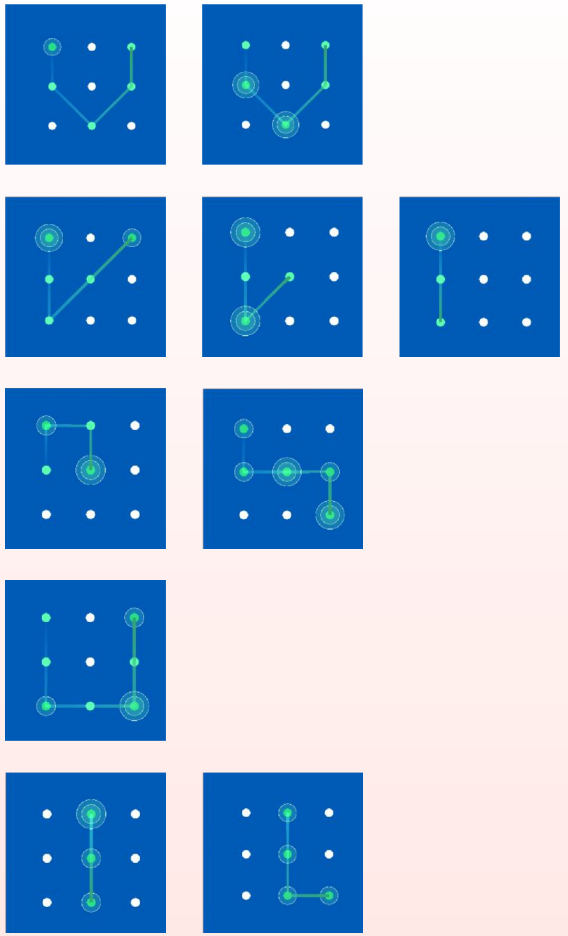
Error Analysis

Table 5 : Common trends in errors - multi hold

The Multi Hold Password Schema:

The trend seen here is that the users found it difficult to control the hold duration between the long and short hold. The time window of 1 sec, was thus proven to be not fit for this type of interaction to have good usability. Users were visibly irritated while entering this password because of this.

Set password	Errors
	

Set password	Errors
	

Error Analysis

The Multi Pattern Password Schema:

Just like multi visit, here also they (users) hastily entered the pattern without hesitancy. repeated strokes were forgetful, and the directionality also proved to be of a challenge. This is probably due to the fact that when having multiple patters users focused on retaining the final image of the pattern rather that actions that led to them.

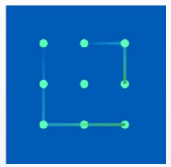
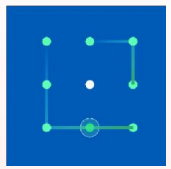
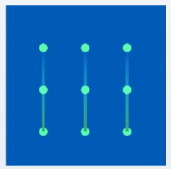
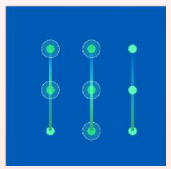
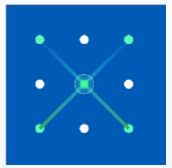
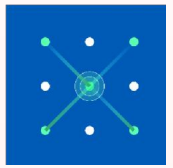
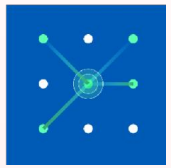
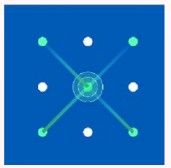
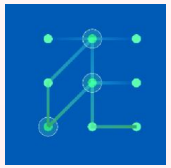
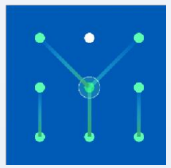
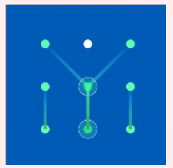
Set password	Errors
	
	

Table 6 : Common trends in errors - multi pattern

Set password	Errors
	 
	  
	  
	

Data Analysis

Password Entropy

Password entropy is a measure of password strength which quantifies the unpredictability and complexity of passwords, directly impacting their resistance to guessing attacks. In the context of pattern-based passwords, diversity refers to the range of distinct patterns users create. A schema with higher entropy and greater pattern diversity is generally considered more secure. To assess this, we could analyze the uniqueness of patterns, the predictability based on common user behaviors, and the resilience against common attack vectors. Incorporating statistical analysis and entropy calculations will provide a comprehensive comparison of the novel password schemas against the benchmark, highlighting their relative strengths and vulnerabilities in terms of security and usability.

We employ the Li and Vitányis's use of the Kolmogorov Similarity measure w.r.t. the research "On Quantifying the Effective Password Space of Grid-based Unlock Gestures" [19]. This approach introduces a similarity metric for evaluating the effective password space of user-defined gestures. It assesses if one pattern can be converted into another through a specific number of steps or changes. They include:

1. Rotation: *Rotating a pattern by 90, 180 or 270 degrees*
2. Translation: *Translating a pattern by 1 point any of the 4 direction.*
3. Mirror: *Mirror a pattern on the x-axis or y-axis*
4. Inversion: *Traversing a pattern sequence in opposite order.*

Data Analysis

Password Entropy

Grouping Patterns

If two or more patterns say A and B are found to be exactly same, then they are assigned the Kolmogorov distance of n=0. The number of operations required to convert B into A gives us the Kolmogorov distance between the two. We limit our analysis to groups of congruent patterns (with equal length), since we consider shapes to be the most important property in the pattern creation process. Also, we limit the analysis to a max distance of n=3.

Next we did greedy clustering of the identified groups of patterns. It involves finding the “best” set of central pattern in the whole dataset of similar patterns manually for this study since we had a limited dataset, and then arranging the related groups in order of distance (n).

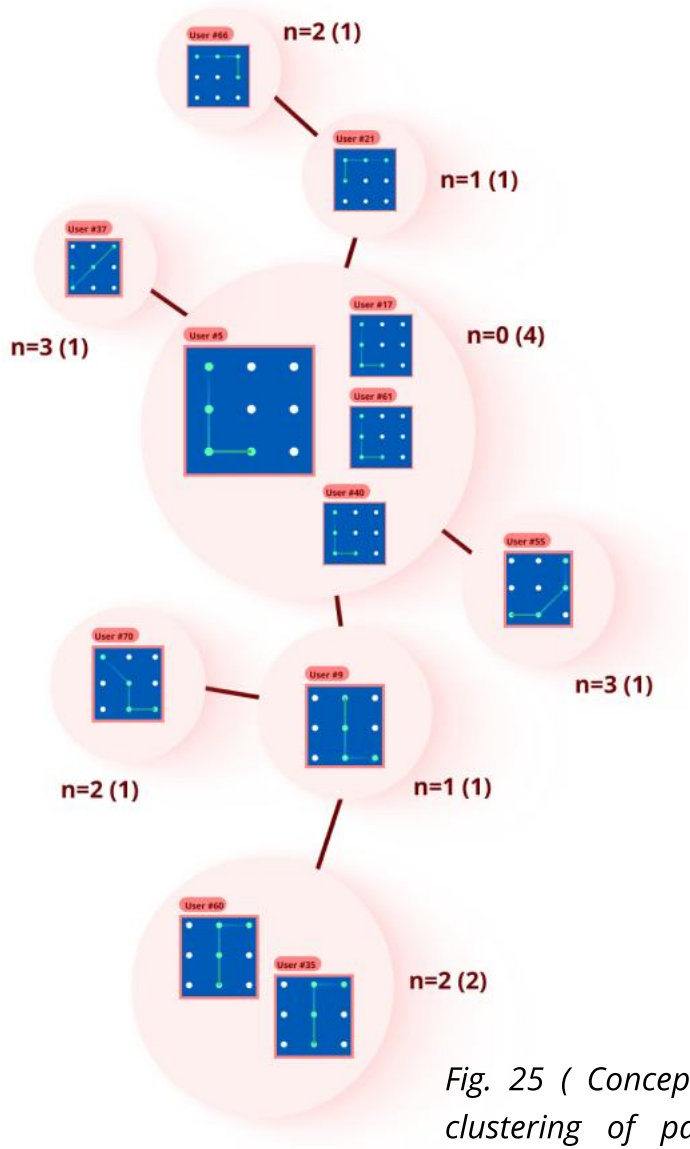


Fig. 25 (Conceptual greedy clustering of pattern data similar to letter ‘L’)

Data Analysis

Password Entropy

The similarity analysis confirms that in the benchmark, the users selected their unlock pattern from a limited set of similar shapes. From the dataset, we deduced that more than half of the patterns set by the users in the benchmark were derived from just 5 patterns with n<=4. The most popular pattern group ('L') had 21 instances (~30%). They were followed by the letters N, S, W & P (~6.8%, 5.5%, 5.5% & 5.5% respectively).

If we remove the exact copies (n=0) the sample space of passwords of 73 reduces to 54 (~73%).

In the novel schemas though the clustering is barely seen. Proving that the proposed password scheme has much higher entropy than the benchmark. In the Multi-Visit schema, out of the dataset of 24, 23 were unique (only one set with n=0). And no set of patterns were related by n=1.

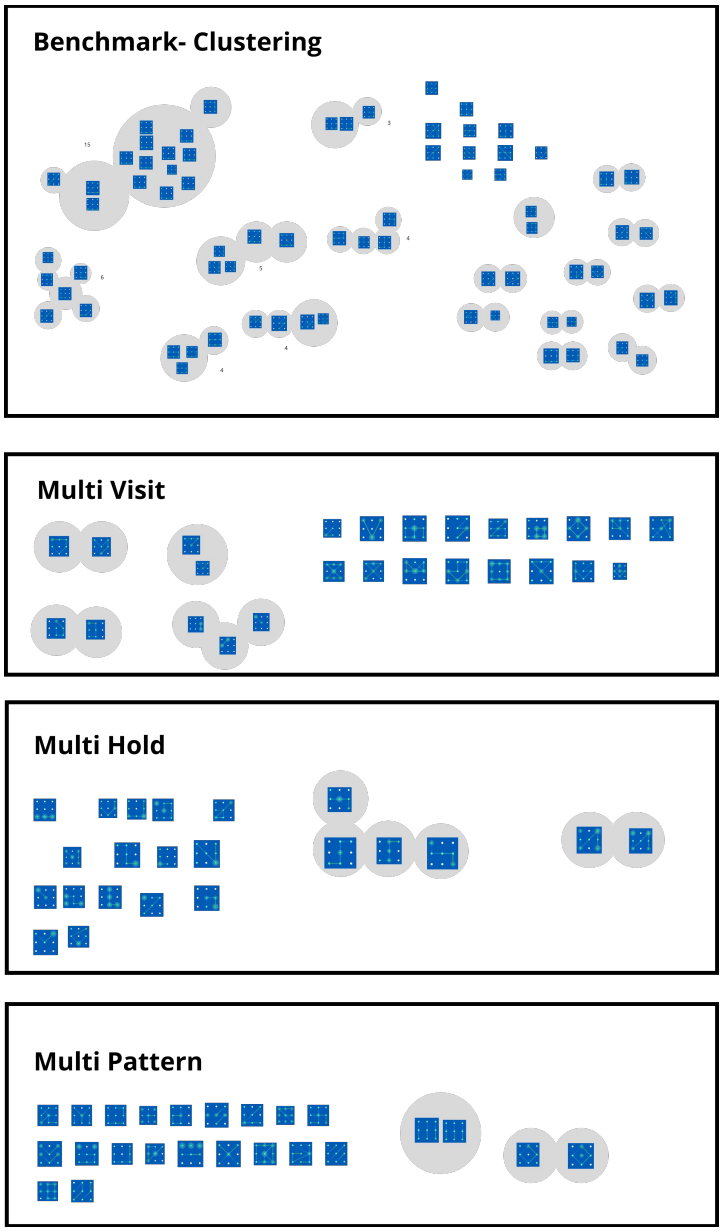


Fig. 26 (Cluster formations of the dataset)

Data Analysis

Password Entropy

Only 4 clusters formed with n=2(2), n=3(1), & n=4(1).

In the Multi-Hold schema, all the patterns were unique. Only 6 patterns were part of a cluster with n=2(1), n=3(2) & n=4(1). In the Multi-Pattern schema, there was only 1 repetition in the dataset (n=0). Out of 24, 23 were unique patterns and only 4 patterns were a part of a cluster.

Data Analysis

Basic Statistics

Since each subject provided with 2 sets of patterns (one benchmark and other the intervention), we have 74 benchmark patterns, 25 multi visit and 24 of each of multi hold, and multi pattern schemas.

Pattern Length:

All the user-generated patterns were analyzed for the number of dots that were engaged with (including repeating dots) out of the 9 dots. Fig. 45 shows the comparison. When we check for significant differences using one-way ANOVA and post hoc Tukey's Honest Significant Difference (HSD) test, we find that people interact with significantly less number of dots in the existing pattern schema when compared to the novel pattern password schemas.

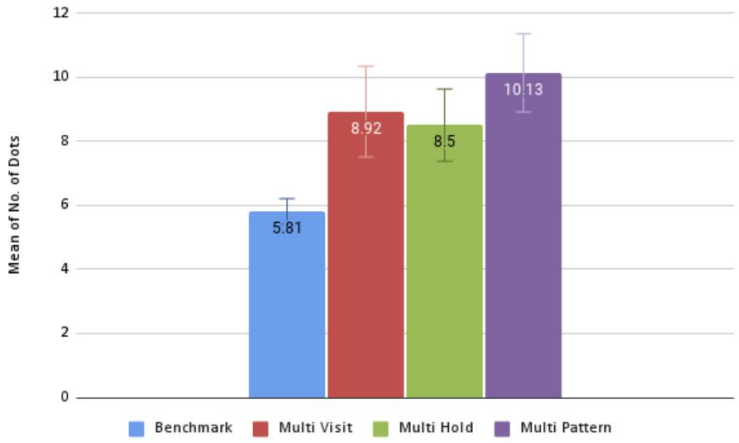


Fig. 27 (Mean number of dots interacted with per pattern)

ANOVA

Lable

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	448.713	3	149.571	23.041	<.001
Within Groups	921.780	142	6.491		
Total	1370.493	145			

Multiple Comparisons

Dependent Variable: Lable

Tukey HSD

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Benchmark	Multi Visit	-3.112*	.590	<.001	-4.65	-1.58
	Multi Hold	-2.692*	.599	<.001	-4.25	-1.13
	Multi Pattern	-4.317*	.599	<.001	-5.88	-2.76
Multi Visit	Benchmark	3.112*	.590	<.001	1.58	4.65
	Multi Hold	.420	.728	.939	-1.47	2.31
	Multi Pattern	-1.205	.728	.351	-3.10	.69
Multi Hold	Benchmark	2.692*	.599	<.001	1.13	4.25
	Multi Visit	-.420	.728	.939	-2.31	1.47
	Multi Pattern	-1.625	.735	.126	-3.54	.29
Multi Pattern	Benchmark	4.317*	.599	<.001	2.76	5.88
	Multi Visit	1.205	.728	.351	-.69	3.10
	Multi Hold	1.625	.735	.126	-.29	3.54

*. The mean difference is significant at the 0.05 level.

Data Analysis

Basic Statistics

Physical Length:

It amounts to the actual physical distance that the user is traversing their finger on the screen to make the pattern. Though the distances may vary from device to device, we use the distance between the two adjacent dots (not diagonally) as one unit. The following graph tabulates the mean of each of the schemas with their error margins of 95% confidence.

As expected the added complexities of multi-hold and multi-pattern discourages the users from traversing their fingers more. The lack of revisit's affordance inhabit users from traversing their fingers longer.

When we check for significant differences using one-way ANOVA and post hoc Tukey's Honest Significant Difference (HSD) test, we find that the Multi Visit Pattern schema is significantly different from the rest due to this fact.

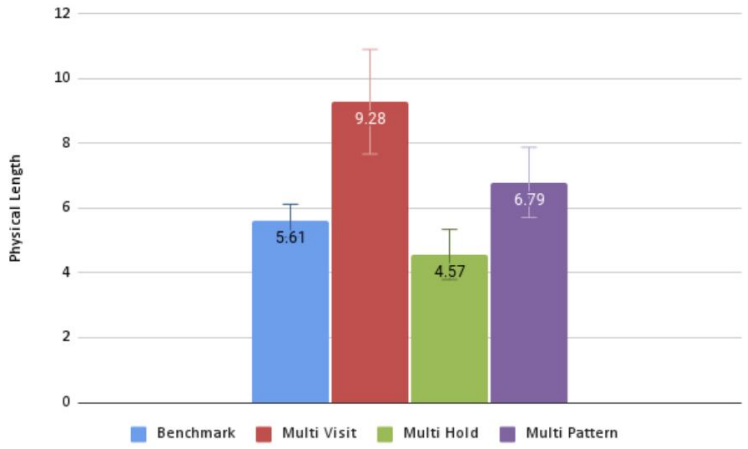


Fig. 28 (Physical length of patterns per pattern)

ANOVA

Lable

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	329.215	3	109.738	15.844	<.001
Within Groups	983.500	142	6.926		
Total	1312.714	145			

Multiple Comparisons

Dependent Variable: Lable

Tukey HSD

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Benchmark	Multi Visit	-3.666770630*	.609852181	<.001	-5.25221202	-2.08132924
	Multi Hold	1.039668574	.619243981	.339	-.57018881	2.64952596
	Multi Pattern	-.972176061	.619243981	.399	-2.58203344	.63768132
Multi Visit	Benchmark	3.666770630*	.609852181	<.001	2.08132924	5.25221202
	Multi Hold	4.706439204*	.752082343	<.001	2.75124004	6.66163837
	Multi Pattern	2.694594569*	.752082343	.003	.73939541	4.64979373
Multi Hold	Benchmark	-1.039668574	.619243981	.339	-2.64952596	.57018881
	Multi Visit	-4.706439204*	.752082343	<.001	-6.66163837	-2.75124004
	Multi Pattern	-2.011844635*	.759717893	.044	-3.98689404	-.03679523
Multi Pattern	Benchmark	.972176061	.619243981	.399	-.63768132	2.58203344
	Multi Visit	-2.694594569*	.752082343	.003	-4.64979373	-.73939541
	Multi Hold	2.011844635*	.759717893	.044	.03679523	3.98689404

*. The mean difference is significant at the 0.05 level.

Data Analysis

Pattern Trends

Preference for the start and end positions. :
In accordance with the to the Fitts's law, and the user's natural reading and writing habits, which typically progress from left to right and top to bottom, there was a trend in the user's choice of the start and end points of the patterns that they created. They predominantly chose the top left and the bottom right dots to start and end their patterns respectively.

A preference for starting and ending dots in pattern locks can significantly reduce the effective password space, making patterns more predictable and susceptible to guessing attacks. This behavioral uniformity among users narrows the range of unique patterns, thereby compromising security by facilitating easier identification of common patterns or trends, which attackers can exploit.

From the user-generated patterns, we tabulated the percentages (frequency in %) of dots that are the beginning (first table) and the end (second table to the right) of those patterns schematically with the following heatmaps.

	A	B	C
1	52.05	6.85	16.44
2	6.85	1.37	2.74
3	10.96	2.74	0

	A	B	C
1	1.37	4.11	9.59
2	2.74	5.48	6.85
3	21.92	8.22	39.73

Fig. 29.1 (Benchmark - % of pattern's start (left) and end (right))

	A	B	C
1	32	20	4
2	4	12	4
3	12	12	0

	A	B	C
1	16	16	8
2	0	16	8
3	8	12	16

Fig. 29.2 (Multi Visit - % of pattern's start (left) and end (right))

Data Analysis

Pattern Trends

	A	B	C
1	70.83	8.33	4.17
2	0	0	0
3	16.67	0	0

	A	B	C
1	0	0	20.83
2	0	12.5	0
3	8.33	4.17	54.17

Fig. 29.3 (Multi Hold - % of pattern's start (left) and end (right))

	A	B	C
1	28.89	13.33	11.11
2	17.78	4.44	4.44
3	8.89	6.67	4.44

	A	B	C
1	4.44	6.67	17.78
2	0	6.67	15.56
3	13.33	13.33	22.22

Fig. 29.4 (Multi Visit - % of pattern's start (left) and end (right))

The schematic representation shows that there is a significant trend in the preference for the edges as start and end points in the benchmark and the multi-hold pattern schema. The hypothesis that one can draw from this data is that maybe the affordance to revisit a dot harms the behavioral tendency of users to use extremes as edges.

Visual Complexity.

To create a more shoulder surfing-proof graphical authentication system from this grid-based lock pattern system, we need to increase the visual complexity of the pattern that the user sets. If the pattern cris-crosses or overlaps at multiple points or lines, then that pattern is also less prone to smudge attacks. Increasing these to factors can greatly enhance the security of the schema, hence we checked from the user-generated database if the proposed schema performs better than the benchmark and if (to what extent) the users are creating more visually complex patterns.

Visual Complexity of patterns in our context can be quantified by factors such as how many cris-crossing of the strokes is happening in the patterns, how many dots are being interacted with more than once, how many strokes are

Data Analysis

Pattern Trends

overlapped, or the number of independent strokes users are creating (in case of multi-pattern) etc. The following points answer these questions.

Fig 45 shows the number of dots revisited or long hold from our user generated data.

The tendency of users to create a pattern that involves a crisscrossing strokes is higher in the Multi-Visit and Multi Pattern schema which have the affordance to revisit a dot. (Fig. 45)

Overlapping strokes in a pattern eliminates the smudge attack susceptibility to a great extent. Users can create such patterns in Multi-Visit and Multi-Pattern schemas. From our data, we found that per patter, there were 2.16 overlapping strokes in Multi-Visit schema (+/-1.32), and 0.125 (+/- 0.18) in that of Multi-Pattern schema.

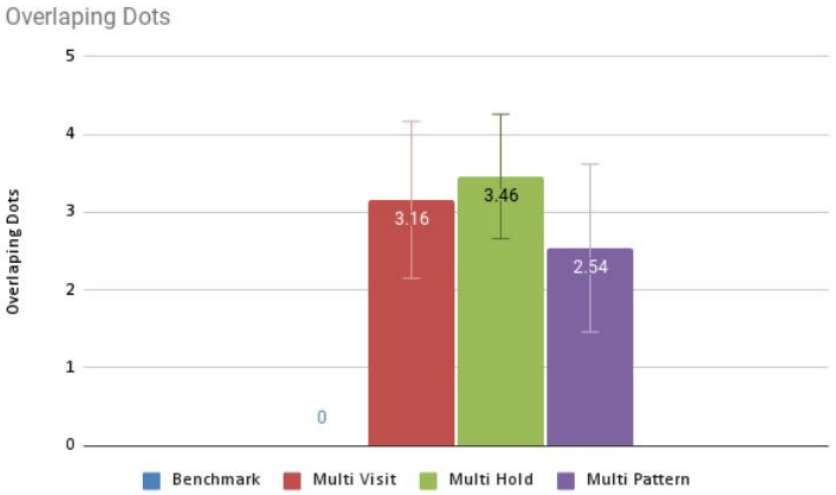


Fig. 30 (Overlapping dots per pattern)

Fig. 31 (criscrossing strokes per pattern)

Data Analysis

Visual Complexity

Multi-Pattern gives the affordance to create more than 1 pattern, on an average, users created 3.875 patterns (+/-0.95) per user.

To quantify the visual complexity factor of the user generated patterns, we refer to the technique used in the paper [19] by the following equation.

$$Vp = Sp \times \log_2\{Lp + \alpha*Cp + \beta*Op + \gamma*Zp + \Delta*(Np-1)\}$$

equation 1

Where Vp is the visual complexity score for pattern p, Sp : Size (number of dots connected in the pattern), Lp : Physical length, Cp : Number of intersections(crisscrosses), Op : Overlapping Dots, Zp : Overlapping Strokes and Np : Number of Strokes.

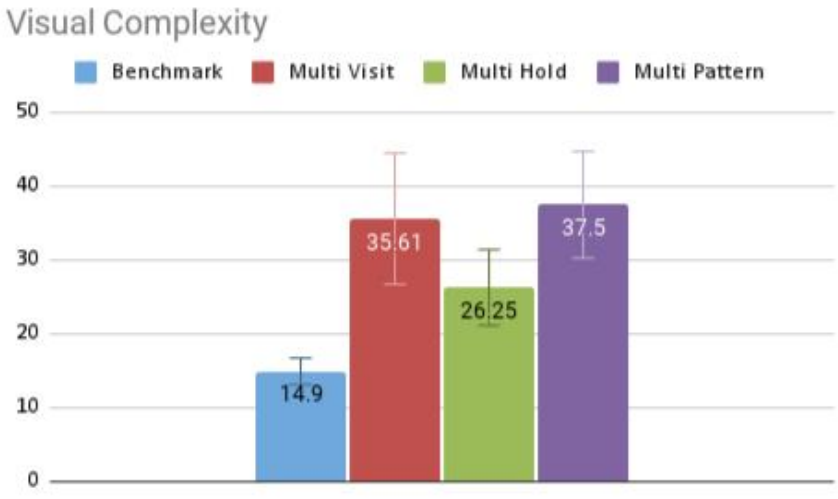


Fig. 32 (Mean Visual Complexity of patterns)

ANOVA

Lable

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13912.457	3	4637.486	24.179	<.001
Within Groups	27235.222	142	191.797		
Total	41147.679	145			

Homogeneous Subsets

Lable

Tukey HSD[a,b]

Group	N	Subset for alpha = 0.05		
		1	2	3
Benchmark	73	14.89977161		
Multi Hold	24		26.24821640	
Multi Visit	25		35.61454074	35.61454074
Multi Pattern	24			37.49905156
Sig.		1.000	.052	.954

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 29.190.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

Data Analysis

Visual Complexity

α, β, γ and Δ are the weights of their respective factors that are required to be deduced by the multi-criteria decision analysis (MCDA) approach for these schemas to have a more accurate quantification of the visual complexities in these password schemas. They are also required to be reflective of the difficulty a brute force password breaking algorithms. here we have taken these weights as α=β=γ=Δ=1.

They subsequent analysis showed that all novel pattern schema's mean visual complexity score are significantly different from the benchmark and the mean visual complexity of Multi Pattern is significantly greater than Multi Hold scheme.

Data Analysis

User Preferences

Employing a between-subjects design, the total sample of 72 participants was evenly divided into three groups, corresponding to each of the proposed password schemas. From each of these groups, a subset of 15 participants was randomly selected, resulting in a total of 45 participants for the survey phase. This selection process ensured that each password schema was evaluated by an equal number of participants, thus facilitating a balanced comparison against the established benchmark. The primary objective was to ascertain the relative user preferences for each schema, thereby providing insights into their usability parameter.

Participants in the study were requested to evaluate each password schema on a scale ranging from 1 to 10, with the benchmark password schema being assigned a baseline score of 5. Subsequent to collecting these ratings, the average scores for each password schema were computed and tabulated alongside their respective error margins, calculated to represent a 95% confidence interval (CI). The results of these calculations, including the average user preference scores and their error margins, are visually presented in the adjoining figure.

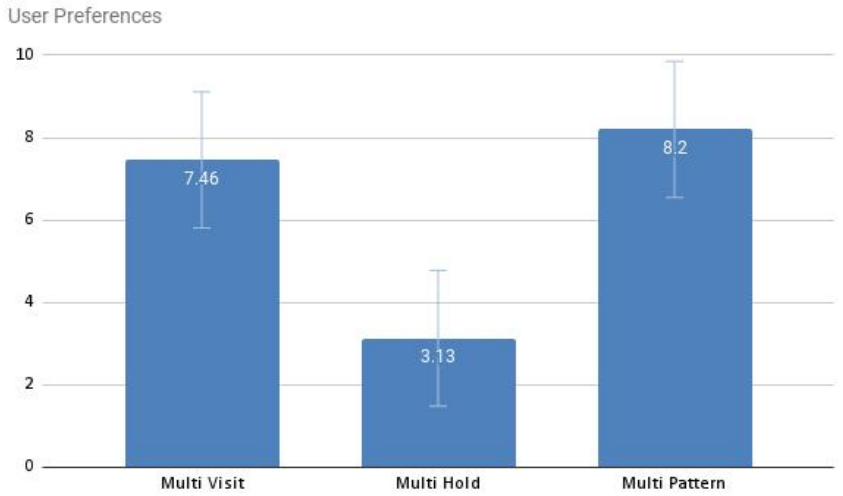


Fig. 32 (User preference score of each novel password schema)

Conclusion

Inferences

Following are the inferences that arise from the collected data in this study.

Inference #1

Impact of complexity on Recall

The study showed a clear relationship between the complexity of the pattern lock system and the forgetfulness. Multi Visit showed similar recall rates as that of the benchmark as it was the least complex amongst all the 3. Multi Hold and Multi Pattern conclusively showed lower recall rates.

Inference #2

High forgetfulness of Multi hold

This study showed that hold type interactions are not very memorable. It's probably because it is difficult to retain and recall the hold duration required for this type of interaction.

Inference #3

Input Time with Complexity and Novelty

The results demonstrate a clear trend where increased complexity or novelty in the pattern lock system correlates with longer input times. The Multi Visit takes approximately 2 seconds longer, Multi Hold about 3.9 seconds longer, and Multi Pattern around 4.5 seconds longer than the Benchmark.

Inference #4

Trade-Off between input times & security

All the password schemas that were put the test took considerably less time than the typical alphanumeric password [17]. The password schemas offers similar password space with the input times slightly more than the existing android pattern locks.

Conclusion

Inferences

Inference #5

Trade-Off between memorability & security.

Hold type interactions are not very memorable. It's probably because it is difficult to retain and recall the hold duration required for this type of interaction.

Inference #6

Error rates in the interactions

The error rates of the novel interactions were found to be more than that of the benchmark (for Multi hold and Multi Pattern) despite the fact that users took longer time to input. This proves that there is a learnability and adaptability curve that the users need to go through before these interactions become accurate if this passwords schema is adopted.

Inference #7

Hold threshold for Multi Hold

It was observed that in the multi hold schema, the users were unable to distinguish between the short and long holds that were of 1 and 2 sec. respectively.

Inference #8

Interaction affordances cause more diversity

It is conclusively proven than the existing pattern schema in the android locks suffers with very low entropy. With the addition of interaction as affordance, we were able to substantially expand upon the password space and users also created more diverse patterns which subsequently increased the overall strength without much addition to the cognitive load.

Conclusion

Inferences

Inference #9

Interaction affordances cause more diversity

It is conclusively proven than the existing pattern schema in the android locks suffers with very low entropy. With the addition of interaction as affordance, we were able to substantially expand upon the password space and users also created more diverse patterns which subsequently increased the overall strength without much addition to the cognitive load.

Inference #10

Start and end preferences in passwords

The generated data conclusively shows that the pattern that are created in the Multi-Visit and the Multi-Hold schemas are less prone to begin and end from the popular positions, hence being less prone to breach.

Inference #11

Visual Complexity score of novel passwords

The generated user data conclusively shows that the visual complexity and hence-forth the resilience against smudge and shoulder-surfing attacks of the password is most in the Multi-Pattern scheme followed by the Multi-Visit, then the Multi-Hold. All three novel schemas are much better than the existing scheme.

Inference #12

User preference of novel passwords

The users disliked the Multi-Hold schema in it's existing from, while the multi-visit and the multi-patters schema were rated more preferably than the existing schema.

Conclusion

Discussions

With the inferences of the collected data and our observations and experiences obtained in this study, we came up with the adjacent graph that conceptually depicts the position of the 4 password schemas on the Security vs Memorability and Usability graph.

The Benchmark though most usable and and lacks the security restricting it's use case to just phone locks. Adding interaction affordances to the schema increases the security exponentially. The Multi Visit schema's tradeoff is the least.

Multi Hold surely offers much more security but it is the least usable and memorable. Users also didn't preferred the interactions.

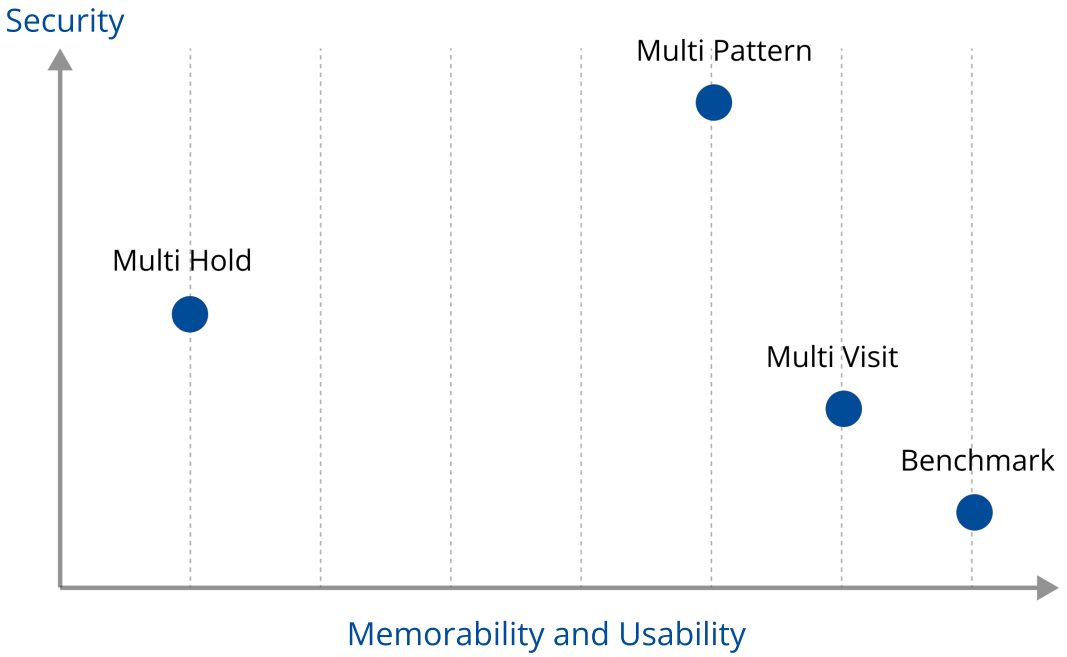


Fig. 33 (Conceptual Diagram)

Multi Pattern schema is the most secure and much more usable / memorable than the multi hold schema. It was also rated much more positively than the rest. It was in our opinion the best amongst the three designed passwords.

Conclusion

Limitations & Future Scope

The study has a **narrow defined set of audience** on which it was tested. Further studies are required to establish if these results are same for different socio-economic-cultural groups.

The designed password schemas can be tested in **different devices** with touch as well as keyboard interfaces like Char Pattern [13] to evolve them into a more versatile solution.

The new designed schemas seems to be harder to guess for the onlooker making it resistant to attacks such as **shoulder surfing**. Further studies are required to quantitively prove if there is a significant improvement in this respect or not.

This study does not takes into account a very important parameter of usability, i.e. the **Cognitive Load Test**. This paper [20] provides the methodology that can be adopted for this context.

References

[1] Ians (2017) Just 5 attempts can open Android Pattern Lock, The Hindu. Available at: https://www.thehindu.com/sci-tech/technology/gadgets/Just-5-attempts-can-open-Android-pattern-lock/article17092221.ece (Accessed: 23 October 2023).

[2] Published by Laura Ceci and 8, D. (2023) Screen lock methods for global mobile users 2021, Statista. Available at: https://www.statista.com/statistics/1305993/screen-lock-methods-global-users/ (Accessed: 23 October 2023).

[3] Andriotis, P. et al. (2016) 'A study on usability and security features of the android pattern lock screen', Information & Computer Security, 24(1), pp. 53–72. doi:10.1108/ics-01-2015-0001.

[4] Ku, Y. et al. (2019) Draw it as shown: Behavioral Pattern Lock for Mobile user authentication, IEEE Access. Available at: https://ieeexplore.ieee.org/document/8721054 (Accessed: 23 October 2023).
vol. 7, pp. 69363-69378, 2019, doi: 10.1109/ACCESS.2019.2918647.

[5] Løge, M.D. (2015) Tell Me Who You Are and I Will Tell You Your Unlock Pattern. dissertation.

[6] Zhang, L. et al. (2021) 'Does the layout of the Android unlock pattern affect the security and usability of the password?', Journal of Information Security and Applications, 62(C), p. 103011. doi:10.1016/j.jisa.2021.103011.

References

[7] https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2015-0001/full/html

[8] Dunphy, P., Nicholson, J. and Olivier, P. (2008) 'Securing pass faces for description', Proceedings of the 4th symposium on Usable privacy and security [Preprint]. doi:10.1145/1408664.1408668.

[9] Joshi, A.M. and Muniyal, B. (2018) 'Authentication using text and graphical password', 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 381–386. doi:10.1109/icacci.2018.8554390.

[10] Group, T. (2021) Grid authentication, Cloud Protection & Licensing Solutions. Available at: https://cpl.thalesgroup.com/access-management/authenticators/grid-authentication (Accessed: 24 October 2023).

[11] Hanif, S. et al. (2019) 'A new shoulder surfing and mobile key-logging resistant graphical password scheme for smart-held devices', International Journal of Advanced Computer Science and Applications, 10(9). doi:10.14569/ijacsa.2019.0100957.

[12] Aviv, A.J., Kuber, R. and Budzitowski, D. (2017) 'Is bigger better when it comes to Android graphical pattern unlock?', IEEE Internet Computing, 21(6), pp. 46–51. doi:10.1109/mic.2017.4180833.

References

[13] Bicakci, K. and Satiev, T. (2015) 'Charpattern: Rethinking android lock pattern to adapt to remote authentication', Technology and Practice of Passwords, pp. 74–86. doi:10.1007/978-3-319-24192-0_5.

[14] von Zezschwitz, E. et al. (2013) 'Making graphic-based authentication secure against Smudge attacks', Proceedings of the 2013 international conference on Intelligent user interfaces [Preprint]. doi:10.1145/2449396.2449432.

[15] Zheng, J. and Chigurupati, S.K. (2019) 'M-pattern: A novel scheme for improving the security of Android pattern unlock against Smudge attacks', ICT Express, 5(3), pp. 192–195. doi:10.1016/j.icte.2018.11.003.

[16] Cho, G. et al. (2017) 'Syspal: System-guided Pattern Locks for Android', 2017 IEEE Symposium on Security and Privacy (SP) [Preprint]. doi:10.1109/sp.2017.61.

[17] Niezen, G. and Hancke, G.P. (2009) 'Evaluating and optimising accelerometer-based gesture recognition techniques for mobile devices', AFRICON 2009 [Preprint]. doi:10.1109/afrcon.2009.5308175.

[18] Mujeye, S. et al. (2016) 'Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity', Online Journal of Applied Knowledge Management, 4(1), pp. 99–116. doi:10.36965/ojakm.2016.4(1)99-116.

References

[19] von Zezschwitz, E. et al. (2016) 'On quantifying the effective password space of grid-based unlock gestures', Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia [Preprint]. doi:10.1145/3012709.3012729.

[20] Mujeye, S. et al. (2016) 'Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity', Online Journal of Applied Knowledge Management, 4(1), pp. 99–116. doi:10.36965/ojakm.2016.4(1)99-116.

[21] Ye, Guixin & Tang, Zhanyong & Fang, Dingyi & Chen, Xiaojiang & Kim, Kwang & Taylor, Ben & Wang, Zheng. (2017). Cracking Android Pattern Lock in Five Attempts. 10.14722/ndss.2017.23130.

References to figures

[Fig. 2] Khan, Wazir & Aalsalem, Mohammed & Xiang, Yang. (2011). A Graphical Password Based System for Small Mobile Devices. International Journal of Computer Science Issues. 8.

[Fig. 5] Zheng, J. and Chigurupati, S.K. (2019) 'M-pattern: A novel scheme for improving the security of Android pattern unlock against Smudge attacks', ICT Express, 5(3), pp. 192–195. doi:10.1016/j.icte.2018.11.003.