PICTURE-BASED PASSWORD SCHEME TO RESIST SHOULDER-SURFING ATTACKS

By

WONG LING CENT

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONOURS)
Faculty of Information and Communication Technology
(Kampar Campus)

FEBRUARY 2026

ACKNOWLEDGEMENTS

I would like to most sincerely thank my supervisor, Mr. Ku Chin Soon, who has given me invaluable guidance, patience, and constant support throughout the period of this project. The support and positive feedback both have contributed to my success overcoming the hurdles I faced and improving the quality of my work.

I would also like to thank my friends who always supported my work and motivated me to be focused and dedicated to the completion of this project.

COPYRIGHT STATEMENT

This Final Year Project proposal is submitted in partial fulfillment of the requirements for the degree of Bachelor of Computer Science (Honours) at Universiti Tunku Abdul Rahman (UTAR). This Final Year Project proposal represents the work of the author, except where due acknowledgment has been made in the text. No part of this Final Year Project proposal may be reproduced, stored, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the author or UTAR, in accordance with UTAR's Intellectual Property Policy.

ABSTRACT

Memorability can be a problem with traditional text-based passwords, and they are quite susceptible to observation-based attacks, including shoulder-surfing. This project introduces GridLock, a new recognition-based graphical password system, which overcomes these limitations by having a directional mechanism resembling a compass that integrates visual object selection with spatial memory. The system was produced as a fully operational Android application based on Firebase with four prototypes that were systematically compared (Compass Pro VIII, Compass Pro IV, Compass Lock IV and Compass Lock VIII). These differences are in compass orientation (dynamic and static) and directional complexity (4-way and 8-way).

The prototypes were tested on three fundamental dimensions: efficiency in registration and logging in, resistance to shoulder surfing, and long-term memorability, using a 7 days longitudinal test. Empirical evidence suggests that the initial usability of a prototype, with the fastest baseline login time (21.38s), was the static 4-directional prototype (Compass Lock IV), although the dynamic prototypes (Compass Pro) initially came with a greater cognitive load. This friction was solved soon though, as users were able to perform at the level of an expert within days. Importantly, serious penetration tests showed that even with full logic disclosure, all prototypes obtained an absolute 0% breach rate, which indicates serious resistance to shoulder-surfing. Through incorporating spatial-directional logic in the graphical authentication, the paper finds it conclusive that it is indeed feasible to develop a workable password system that is able to solve the conventional trade-off between security, memorability, and usability.

Area of Study: Information Security and Authentication Systems

Keywords: Graphical Passwords, Compass-based Authentication, Shoulder-surfing Resistance, Mobile Application, Recognition-based Authentication, Spatial Memory

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RGP	Recognition-Based Graphical Password
UI	User Interface
UX	User Experience
ERD	Entity Relationship Diagram
IDE	Integrated Development Environment
XML	extensible Markup Language
SDK	Software Development Kit
PIN	Personal Identification Number

CHAPTER 1

Introduction

Graphical password systems are a type of authentication that uses images or graphics; this makes it easier to remember than conventional passwords based on text. Such systems are especially useful in the visual memory. Graphical passwords have been categorized into three general categories recognition-based, recall-based and cued recall-based. The project will be devoted to recognition-based graphical passwords where users have to identify and select two preset pictures and directions.

Graphical Passwords have been suggested as a simpler tool in order to help overcome these challenges. Nonetheless, the prevailing designs either focus on a single aspect of authentication such as the identification of a still picture or recall of a sign, and they fail to utilize the human spatial and directional memory so as to improve product security [17]. This has left many graphical password systems prone to observation attacks and without the information complexity to be data secure against brute-force attacks related attacks. Besides, previous studies tend to consider only short-term performance factors, and not the long-term memorability and performance under recurring use [3], [5].

To fill these research gaps, this project proposes an new graphical password prototype to be generated and implemented directly on Android platform to make the experimental set-up as close to the real life setting as possible. This prototype will focus on dynamic grid layouts and direction-based authentication mechanism; this is to provide an intuitive, yet hard to crack authentication mechanism. This study will critically assess its performance on some of the key dimensions like registration and log in efficiency, shoulder-surfing resistant and long-term memorability. Such research will yield novel empirical findings regarding trade-offs in the design of graphical passwords, and offer practical solutions toward creating efficient, secure and sustainable graphical password systems, especially on mobile devices.

1.1 Problem Statement

Current textual passwords can be very challenging in terms of balancing usability, memorability, and security. Passwords in the form of texts can be easily forgotten, subject to observation attacks like shoulder-surfing, and needs to be reset often, irking the user and lowering productivity. Despite alternative authentication schemes based on graphical passwords, most current implementation accounts focus on a single feature of authentication e.g. ease of recognition or password strength and fail to consider **trade-offs between efficiency, attack resistance, and long-term recall.** An example can help to clarify this, Passfaces demonstrated high memorability levels, but the system was found to be susceptible to observation attacks, but grid-based systems were more secure, at the cost of reduced usability as more mental work was required [3]. These discrepancies mean that there is no design that has yet been able to be excellently integrated in terms of usability, security, and memorability.

In addition, short term usability and login performance has been extensively investigated, whereas **long-term memorability and systematic anti-shoulder-surfing resistance has not been researched thoroughly.** The use of randomized grids and dynamic location of images has been considered previously as a counter mechanism to observation, although few empirical studies have investigated the value of directional or spatial memory processes in improving security and usability.

Hence this project addressed these gaps by critically assessing recognition-based graphical password prototypes based on dynamic grid layouts and compass directional input. This study measured three performance indicators.: (1) usability in the registration and efficiency in logging in, (2) protection against shoulder-surfing attacks, and (3) memorability during a 7-day longitudinal study.

1.2 Project Motivation

In the digital era, the college population, in particular, the main audience of Internet and mobile devices, perform daily tasks to log in on the learning, social, and financial websites. But with conventional passwords, those based on text, students would always find the passwords troublesome, subject to guessing and very vulnerable to shoulder-surfing. Current research has pointed out the flaws of traditional passwords in usability and security especially within the real-world situation settings such as the library and classroom settings [13], [16]. In addition, the demand to reset lost or forgotten passwords interrupts everyday routines and has an adverse effect on learning and personal productivity.

The drive to come up with this project was inspired by the rising need to have authentication systems that promote usability, security and memorability at the same time. Textual passwords are easy to forget and reuse and are vulnerable to attacks that exploit the user such as shoulder-surfing, whereas graphical password schemes tend to focus on usability at the sacrifice of security. There is still an urgency to find alternative authentication methods, which exploit spatial and directional memory better to use human beings to create more secure and easy methods [17].

This study deployed the implemented system on the Android platform, so the experiments are done in conditions that are relevant to the real-world situation [1]. In this way, the paper emphasizes practical assessment as opposed to desk-based simulation studies that are not entirely practical. Specifically, the project has evaluated the following three key factors: efficiency of registration and logging in [13] protection against shoulder-surfing attacks [8], [9] long-term memorability [3], [5].

By conducting rigorous user studies on the preference and security of numerous prototypes with varying compass locations and granularity in directions, the study contributes empirical findings regarding the trade-offs between usability and security of graphical password design [9]. The findings of this project provide critical insights for the design of authentication systems in the future, which are both resistant to those threats familiar to observations as well as practical to use every day in the long run.

1.3 Research Objectives

1. To evaluate the usability of dynamic grid layouts with directional authentication-based graphical password prototypes by analysing registration time, login time, and success rate.

2. To assess the security against shoulder-surfing attacks through controlled observation tests, investigating the effectiveness of the directional mechanism in resisting cracking attempts.

3. To analyze long-term recall by conducting a 7-day longitudinal study, determining changes in login performance and error patterns to establish user memorability trends.

1.4 Project Scope

This project is focused on the design of a recognition-based graphical password system whose design is intended for university students. An Android-based prototype, GridLock, was developed featuring a dynamic grid layout and direction-based authentication model to effectively improve the resiliency against shoulder-surfing attacks. The research includes prototyping the real system, creating various libraries of images (e.g., everyday objects, animals, flower) and conducting a series of user studies. The primary areas of focus were the following:

- Usability - Measuring registration and login efficiency, findability, and success rates.
- Security - Testing resistance against shoulder-surfing and observation attacks
- Memorability - Assessing password recall accuracy and patterns over a 7-day period.

The user population for the study was limited to university students, and the authentication scheme was limited to directional recognition-based graphical passwords. Other authenticating schemes such as text passwords, biometric or gesture-based schemes will not be considered in this project. Likewise, testing in big fields or cross-platform, or longer than 7 days for memory will be constrained also.

1.5 Contributions

This study provides significant impacts at academical, individual, community and international levels. Academically, it delivers empirical evidence on the trade-offs encountered by recognition-based graphical password systems, namely between usability, memorability, and security. The project demonstrates how the spatial memory in terms of usable security by adding a new directional mechanism that takes into consideration the compass-based input. What is more the work establishes benchmark data on registration and login performance, shoulder-surfing resistance, and long-term memorability. These findings can be useful sources of information, in the future research in the authentication and usable security.

At the individual level, the developed system improves the user experience by allowing a finder-friendly, more resistant to observing, and less-needing-of-periodic-reset password method of login. This decreases the mental and physical load on students and regular digital programs users, particularly where shoulder-surfing is more of a common danger, like in a classroom, library or train.

Societally and industrially, the project promotes useful in sensitizing the masses on the importance of following secure authentication measures by providing an alternative to weak text-based passwords. It is possible that the suggested approach will be implemented in the fields where the secure and easy-to-use authentication is essential, which may be education, online shopping, internet banking, and mobile apps. Moreover, it can be applied to government and enterprise systems, in which confidential data must be well secured without compromising the accessibility of a significant population of users.

Globally, the project addresses the universal challenge of weak passwords. By bridging the gap between academic theory and practical implementation, GridLock contributes to the international standards of usable security, potentially reducing global cyber threats related to password observation.

1.6 Report Organization

This report is organized into five chapters that give a broad overview of the developed system of GridLock and its evaluation. Chapter 1 (Introduction) sets out the basic background to the project. It contains the problem statement and motivation for this research, the definition of the key project objectives, the scope and direction of the work and the foreseen contributions. Chapter 2: Literature Review provides a comprehensive literature review of previous work and systems which are relevant to graphical passwords. This chapter identifies the current gaps in research that exist which this project intends to fill. Chapter 3: Proposed Method/Approach describes the approach and technical aspects of the project. It outlines the system requirements, architecture and design of the different authentication prototypes. Chapter 4 - Preliminary Work describes initial development and implementation work. This paper discusses the design and preliminary results of the system. Chapter 5: Conclusion summarises the major findings of the project, assesses the results and indicates directions for future work.

CHAPTER 2

Literature Reviews

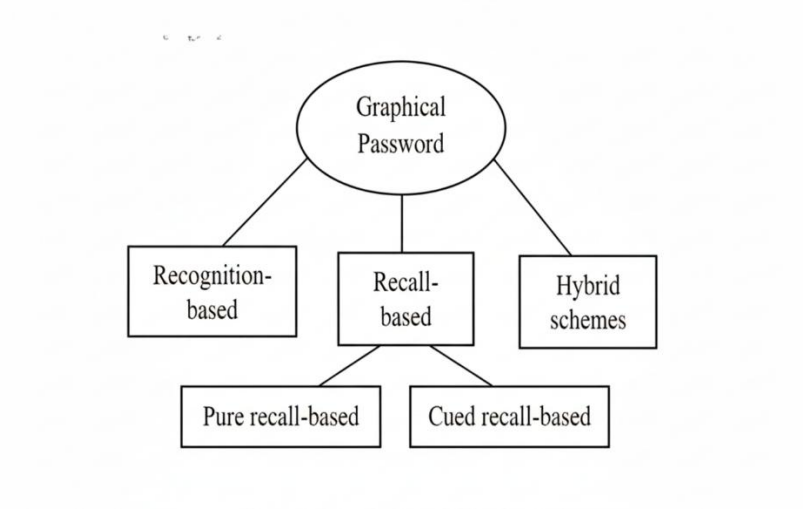


Figure 2.0 Graphical Password System Taxonomy

Graphic password systems based on recognition have received widespread attention in recent years, and related research mainly focuses on the usability, security and memorability of the system. Literature shows that login time, success rate and user feedback are the core indicators for evaluating the effectiveness of the system, while designs such as dynamic grids and image arrangement can help improve security, especially in defending against shoulder surfing attacks. At the same time, different image types and user training methods will also affect the memory effect of passwords and user experience. By combing through existing research, we can provide a theoretical basis and improvement direction for the system design and experimental plan of this project.

2.1 Usability Testing in Recognition-Based Graphical Passwords

Recognition-based graphical password authentication systems get their effectiveness and user-centeredness evaluations through usability tests. Extensive research on usability dimensions such as login time and success rate and user feedback together with user interface design has been conducted to determine security-interface user experience alignment.

Recent studies on recognition-based graphical password systems have mainly concentrated on usability testing, which compares the factors of the success rate of their logins, the efficiency of logins, and the degree of user satisfaction. At least ten reviews and their usability results are discussed in the subsections that follow.

Table 2.1 Summary of Usability Testing Results

No.	Study	Login Time	Login Success Rate	UI Design
1.	A. P. Zuha et al. (2025) [3]	87s	77%	face-image based
2.	P. Ray et al. (2023) [1]	24.19s	94.99%	grid-based
3.	P. Ray et al. (2023) [2]	9.61 ~ 14.56 s	94.80%	background image
4.	Dhanush kumar Ratakond et al. (2022) [26]	87s	93%	background image
5.	I. Sharma and A. Joshi (2025) [27]	20.78~46.10 s	96.91~98.97%	grid-based
6.	H. Sun et al. (2015) [28]	7.27s	95.48%	app icons
7.	M. Harshini et al. (2021) [30]	8s	91%	Segment
8.	S. Azad et al (2017) [29]	10s	89%	Grid-based
9.	H. Alsaiari et al. (2016) [31]	24.5s	93%	grid-based
10.	J. P (2019) [32]	46.03s~63.43s	90.9%	grid-based

Table 2.1 provides a summary of the usability performance of the latest recognition-based graphical password systems with respect to mean time of login, success rate of a login, and interface design. As indicated in the table, grid-based systems, like those of Ray et al. (2023) [1] and Sharma and Joshi (2025) [27], with rather high (more than 94) success are relatively slow in terms of grid density and task specificity, with node login times ranging between 20 seconds and more than 40 seconds. Background image-based schemes, on the contrary, report a higher memorability but tend to need more interaction time, e.g. 87 seconds of a login system described by Zuha et al. (2025) [3].

It is important to note that the lightweight designs such as Sun et al. (2015) [28] that have been applied with familiar app icons show quicker performance in the form of quicker login (7.27 seconds) with the high success rates, which means that interface familiarity might enhance both the efficiency and usability of the interface used.

Altogether, the evidence suggests that recognition-based graphical password schemes may be rather successful, but there is a great discrepancy in the time of the logins across designs. This points to a usability gap to strike equilibrium between speed and accuracy, which is a key impetus to the current study.

2.1.1 Login Time and System Efficiency

System login time functions as an essential measurement to assess the operational speed of graphical password security platforms. Research shows that speed and security levels always maintain a direct relationship in system operations. The SmartGP system [1] integrates smartwatch-based two-factor authentication while users spend an average time of 24.19 seconds to log in. The security increase because of this system justified the reduced speed when compared to traditional PIN entry. The object detection method utilized by GPOD [2] through YOLOv3 algorithm provided fast login times between 9.61 and 14.56 seconds with a high success rate of 94.8% due to its automated design.

The efficiency of logging into systems depends heavily on user knowledge about the images they recognize. Studies [3] demonstrate celebrity-based images lead users to identify them in 45 seconds which outperforms generic Passfaces (87 seconds). This supports research that familiar personal images ease identification through reduced cognitive complexity.

2.1.2 Success Rate and Reliability

The success rate which measures authentication reliability experiences substantial growth when systems employ contextual memory or sensory cues in their design. Users obtained an ~80% success rate after familiarization with the PassPage system [4] by using their browsing history as an authentication element. The successful authentication rate increased to 98% with the “Impact of Cues and User Interaction on The Memorability Of System-Assigned Recognition-Based Graphical Passwords” [5] because it merged spatial and verbal cues throughout one week of trial. The use of descriptive labels paired with systematic arrangement of design elements allowed users to better memorize and retrieve their passwords effectively. The experimental outcomes demonstrate why it is essential to implement fundamental cognitive psychology techniques which improve both password retrieval and decrease authentication mistakes.

2.1.3 User Feedback and Satisfaction

Several organizations use user feedback to confirm the utility of their security systems. Users in “Novel Graphical Password Authentication Scheme with Improved Usability” [6] evaluated a minimalist graphical password system with high "very good" ratings based on ISO 9241-11 criteria because they found it simple to use and its visual organization was clear. Users expressed positive opinions in “The Use of Graphical Password to Improve Authentication Problems in E-Commerce” [7] about abstract inkblot features because they found the system easy to use and useful while also being memorable. Customers asked for larger image grids during requests which demonstrated a requirement for customization options. User satisfaction embraces both system functionality and the capability of personal customization as well as interface flexibility according to research feedback.

2.1.4 User Interface (UI) Design and Interaction Models

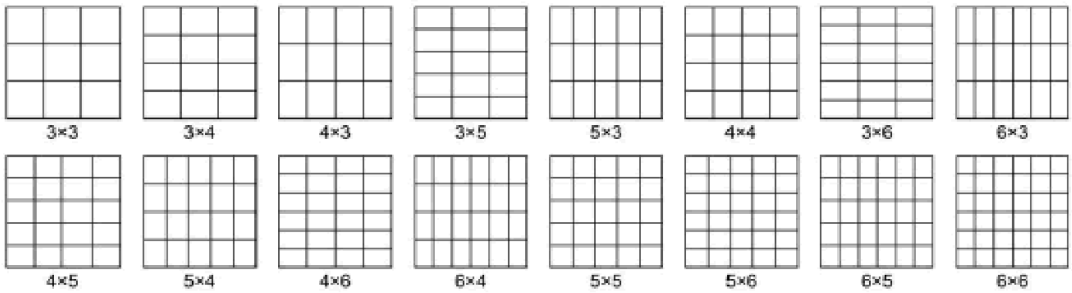


Figure 2.1.4 Different grid formation

Graphical password systems typically employ grid-based layouts due to their intuitive structure. In the study titled "Deep learning based graphical password authentication approach against shoulder-surfing attacks" [8], "PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records" [5], and "Graphical passwords: Behind the attainment of goals" [9] utilize image matrices (e.g., 3x3, 4x4), which mimic familiar smartphone galleries and reduce learning time. For example, Behind the attainment of goals [9] implemented randomized image shuffling within a grid to counter shoulder-surfing attacks while maintaining usability.

Beyond grids, hybrid interfaces are emerging. As discussed in "Eye-tracking-based systems" [10] achieved a 90% success rate using gaze interaction, though they required specialized hardware. Similarly, 3D spatial interfaces [11] increased password strength by 40%, albeit with longer login times. These systems appeal to niche use cases such as accessibility or high-security domains, where conventional UI designs may fall short.

2.2 Security Testing in Recognition-Based Graphical Passwords

Security functions as a fundamental element in recognition-based graphical password (RGP) systems that need to defeat numerous security attacks without compromising accessibility features. The assessment of vulnerability to attacks including shoulder surfing along with brute-force intrusion and phishing and smudge attacks defines security testing within this domain. Research use password entropy along with spoofing accuracy and impersonation resistance measurements to determine how secure a system really is.

To give a concise overview of the security performance of the available recognition-based graphical password schemes, the table below summarizes at least ten studies who tested their effectiveness against typical security threats. The comparison compares against various key types of attacks such as shoulder-surfing attacks, brute-force attacks, dictionary attacks and replay attacks. This synthesis allows a simple comparison of the way various designs against these threats are mitigated and provides information as to their overall efficacy in authenticating situations in the real world.

Table 2.2 Summary of Security Test Results from Existing RGP Schemes

No.	Study	Shoulder-Surfing Resistance	Brute-Force Resistance	Dictionary Attacks Resistance	Replay Attacks
1	N. I. Dias et al. (2023) [8]	Not Mention	Fully Resist	Fully Resist	Not Mention
2	A. Vaddeti (2020) [9]	Fully Resist	Fully Resist	Partial resist	Partial resist
3	S. Lavanya et al. (2019) [33]	Fully resist	Partial resist	Partial resist	Not mention
4	M. N. Al-Ameen et al. (2015) [5]	Partial resist	Partial resist	Partial resist	Not mention
5	Z. Li et al. (2018) [10]	Fully resist	Partial resist	Partial resist	Partial resist

6	B. O. ALSaleem et al (2021) [12]	Fully resist	Fully resist	Partial resist	Not mention
7	A. F. Rasheed et al. (2023) [14]	Fully resist	Fully resist	Fully resist	Partial resist
8	K. Anjitha et al. (2015) [15]	Fully resist	Fully resist	Fully resist	Fully resist
9	H. M. Aljahdali et al. (2014) [16]	Partial resist	Partial resist	Not resist	Not mention
10	W.-C. Ku et al. (2015) [17]	Fully resist	Partial resist	Partial resist	Partial resist

Table 2.2 shows the recent graphical password schemes relying on recognition as well as the resistance of the scheme to most of the security threats such as shoulder-surfing, brute-force, dictionary, and replay attacks. As indicated in the table, other designs exhibit extensive resistance on all categories, e.g. the scheme by Anjitha et al. (2015) [15], that completely resisted all four attacks. According to more recent works, including Rasheed et al. (2023) [14], resilience was also high, but replay attacks were not completely avoided. Conversely, previous studies such as Al-Ameen et al. (2015) [5] and Aljahdali et al. (2014) [16] only offered partial or limited resistance especially against dictionary and replay attacks and as such, they are weaker security models.

Altogether, the evidence shows that although the progress in graphical password schemes is great, in comparison to brute force and shoulder-surfing attacks, the scheme is still vulnerable to dictionary and replay-based threats. This underscores the need to refinements of recognition-based designs, especially about guaranteeing protection of high strength, though without compromising usability.

2.2.1 Resistance to Shoulder Surfing and Observation Attacks

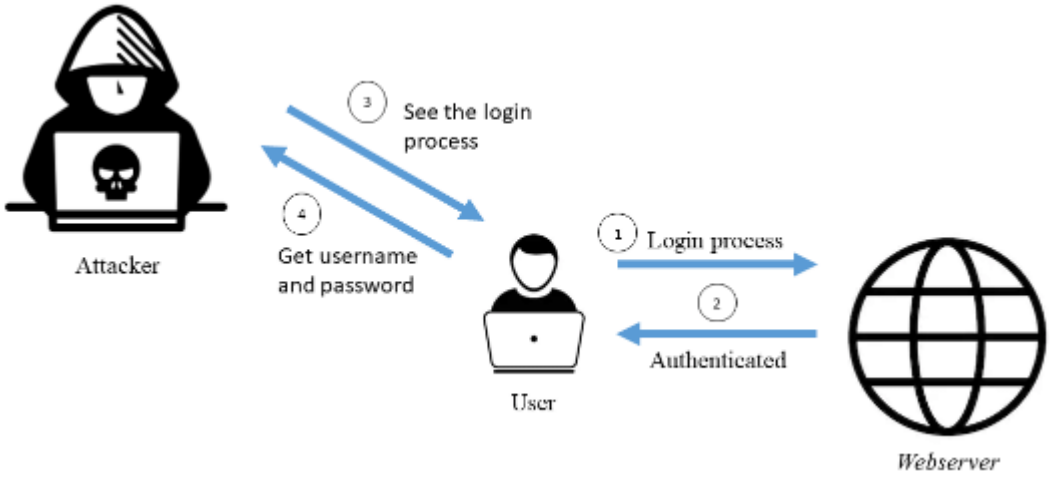


Figure 2.2.1 Shoulder Surfing Attack Illustration

Visual observation as a technique of interference known as shoulder surfing (Figure 2.2.1) presents a continuous threat to the security of graphical password systems. Different counter approaches have been implemented to prevent this threat. The grid-based scheme in Behind the Attainment of Goals [9] produced random image rearrangements during login which made captured authentication sessions invalid before attempting another attack. "The security approach of Multi-Factor Authentication to Systems Login" [12] integrated multiple authentication factors (MFA) by using SMS verification codes with graphical passwords. The method functioned as an added security measure regardless of whether someone was watching the graphical selection process occur. Users of static grid systems such as A Preliminary Study to Evaluate Graphical Passwords for Older Adults [13] faced high observation risks because older individuals frequently selected images that were either recognizable or easily differentiable. The research shows that dynamic interface designs outperform static interface designs when they need to minimize shoulder surveillance threats.

2.2.2 Brute-Force and Automated Attack Resistance

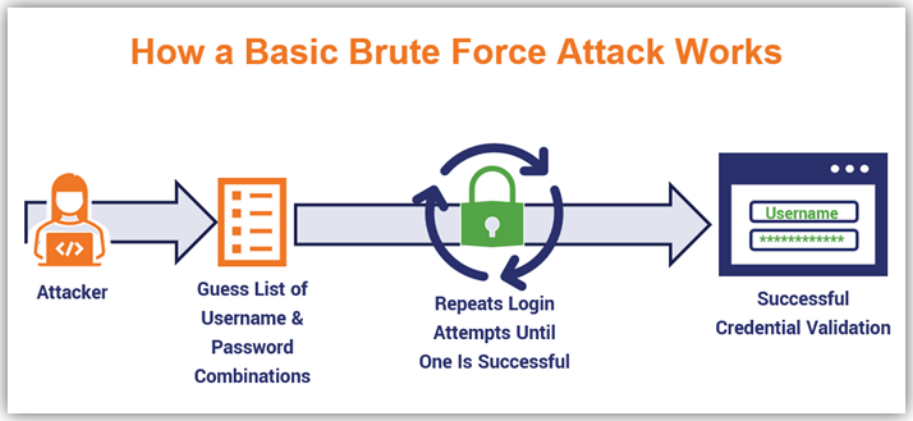


Figure 2.2.2 Brute-Force illustration

The graphical password approach is vulnerable to both brute-force(Figure 2.2.2) and automation-based assault methods. According to Enhancing Graphical Password Authentication System with Deep Learning-Based Arabic Digit Recognition [14] implemented both entropy checks, and selective pixel (SP) optimization features to achieve maximum randomness and limited image data transmission. The decrease in vulnerability made brute-force attacks much more difficult to perform. As discussed in "Captcha as graphical passwords-enhanced with video-based captcha for secure services" [15] implemented CAPTCHA-based distorted images for graphical passwords (CaRP) as its main approach. The spoofing detection approach reached 92.5% success by making automated attacks challenging yet allowing humans to use the images effectively.

2.2.3 Phishing and Social Engineering Vulnerabilities

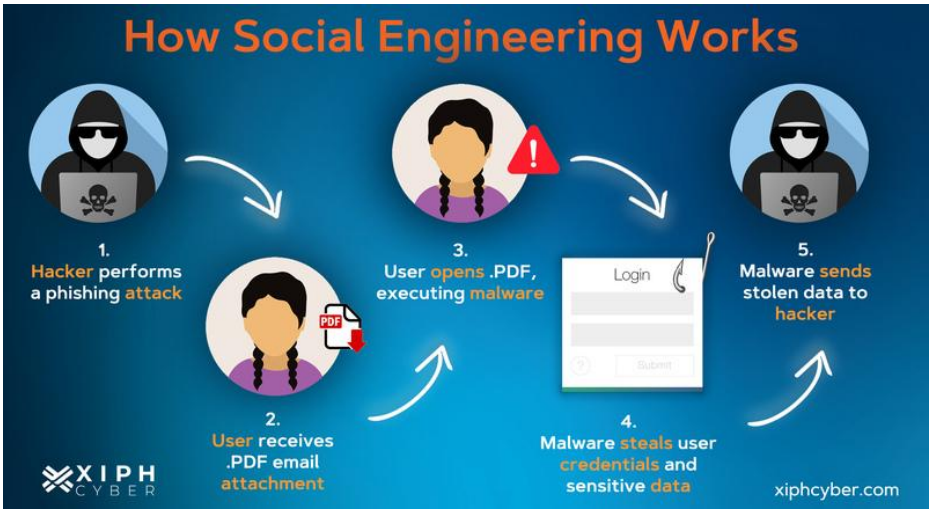


Figure 2.2.3 Social Engineering Vulnerabilities illustration

Phishing (Figure 2.2.3) dangers work by taking advantage of the human elements in authentication procedures. In the study titled “Educated guessing attacks on culturally familiar graphical passwords using personal information on social networks” [16] based authentication security on images which users found culturally familiar or personally associated so attackers could easily manipulate those systems through social engineering methods. Attackers used users' social media profiles to identify the images they selected which usually reflected their personal interests such as sports teams and favourite celebrities or national symbols. The system security level suffered a negative impact because users could predict certain elements. The problem can be resolved through randomized image collections together with abstract visual representations to decrease the occurrence of socially influenced entries that lead to vulnerable credentials.

2.2.4 Quantitative Security Metrics and System Robustness

The assessment methods based on quantitative resistance metrics enable organizations to measure the strength of their systems objectively. Password entropy together with password space size stand as essential security indicators for evaluation. A sector-based graphical password scheme with resistance to login-recording attacks [17] implemented the sector-based dynamic complexity system (RiS) that adapted password challenges based on evolving threat patterns thus boosting the security through increased entropy and problematizing recording attacks. The CAPTCHA-like structure of "Captcha as graphical passwords" [15] provided high spoofing protection along with good defence protocols. The research described in "A gaze gesture-based user authentication system to counter Shoulder-surfing attacks" [18] investigated authentication methods through gaze tracking technology that tracked unique eye movements among users. The authentication systems successfully defeated video recording attacks by maintaining 99% accuracy when calibrated properly and they maintained 96% accuracy when operating with perturbed conditions.

2.2.5 Common Vulnerabilities and Mitigation Strategies

Recognition-based schemes benefit from technological growth, yet they still encounter specific system weaknesses. Hotspot issues persist when users repeat their password selection of particular image elements such as smiling faces in "A Preliminary Study to Evaluate Graphical Passwords for Older Adults" [13] which makes their passwords easier to guess. Sexual orientation and religious preferences exhibited in "Educated guessing attacks on culturally familiar graphical passwords using personal information on social networks" [15] deteriorate both security standards and random authentication principles. The paper titled "Behind the attainment of goals" [9] implemented randomized tap zones to prevent the exposure of touch screen patterns because of smudge residue because traditional numeric PIN methods use predictable entry points.

2.2.6 Key Insights and Future Research Directions

Security enhancement requires interfaces that are both dynamic and randomized accompanied by multi-factor security protocols according to studies. The benefits of personalized security delivery come with a drawback since it affects unpredictability in ways that require maintaining equilibrium. Research indicates that security systems which unite RGP technology with biometric authentication [19] or temporary passwords have resulted in successful outcomes. The field of authentication security now focuses on two research streams: system authentication which adjusts security parameters based on detected conditions and behavioural analytics like keyboard movement and mouse patterns for enhancing security. Thirdly the suggestion of anti-phishing education seeks to prevent users from selecting passwords that follow predictable patterns or are based on social engineering methods.

2.2.7 Compass-Based Authentication: Spatial Information Improving the Security with Directional Indicators

Based on the study on graphical password systems, compass-based authentication involves creating additional element of direction to the submitted point, whereby improving security. As shown by schemes such as the "Sector-Based Textual-Graphical Password" [25], asking a user to perform a spatial or directional decision rather than merely identifying an image makes a big difference in improving password security against shoulder-surfing. Since such an approach is dynamic and randomized, recorded patterns of logins are useless to the attacker, since the reference north may vary with each session. Using the spatial memory is safer and more intuitive since it provides a more secure experience in terms of user interaction.

2.3 Memorability Testing in Recognition-Based Graphical Passwords

Solid memorability stands as a basic requirement for creating recognition-based graphical password (RGP) systems. Unreliable memory recall will cause any security systems based on authentication to become ineffective for real-world applications. Research communities have researched password memorability through multiple approaches including long-term study analysis and cognition assessment and authentication failure examination to determine the factors influencing long-term password recall.

Table 2.3 Summary of Memorability Testing Results

No.	Study	Memorability Findings	Limitations
1	N. I. Dias et al (2023) [8]	High short-term recall	High cognitive load
2	X. Chu et al. (2020) [4]	Good short-term, weak long-term	Decline after 1 week
3	A. H. Shnain et al. (2019) [7]	Better than text passwords	Poor multi-account recall
4	C. Katsini et al. (2019) [20]	User images improved recall	Security trade-off
5	Z. Li et al. (2018) [10]	High recall in lab	Low distraction tolerance
6	A. Constantinides et al. (2021) [34]	Promising memorability	Low precision
7	A. Constantinides et al. (2019) [35]	Better recall with personalization	Privacy risk
8	Y. L. Ho et al. (2022) [36]	Strong recall advantage	Lacks security testing

9	P. Jittibumrungrak et al. (2019) [13]	Recalls dropped after 2 weeks	No reinforcement
10	C. Katsini, et al. (2018) [11]	Dense grids improved recall	Increased login time

Table 2.3 gives an overview of the recent research on memorability with recognition-based graphical passwords. There are also high short-term recall benefits over text passwords (e.g., Shnain et al., 2019 [7]; Ho et al., 2022 [36]), but long-term retention often shows a significant decline as early as the first week (Chu et al., 2020 [4]; Jittibumrungrak et al., 2019 [13]). Personalization or dense grids can enhance recall with some designs (Katsini et al., 2018 [11]; Constantinides et al., 2019 [35]) but at the cost of usability or security. Overall, the available evidence establishes positive effects on memorability but emphasizes the shortage of longitudinal studies in the context of the real world.

2.3.1 Long-Term Retention and Familiarity

Memorability improves through familiar and culturally relevant memorandums based on the results of conducted longitudinal retention tests. Research from "Graphical Passwords for Emergent Users: A Four-Day Recall Comparative Study on PIN, Passfaces and Celebrities" [3] proved that people who chose celebrity faces achieved a 93% success rate at remembering passwords after four days but the Passfaces generic method only reached 77%. The recognition process happens more easily when neural pathways linked to famous faces are already established in the memory. Users who chose culturally relevant images for their security profiles encountered only half as many authentication failures as participants who used images from foreign cultures according to "The Effects of Culture on Authentication Cognitive Dimensions" [24]. The study in "The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords" [5] demonstrated that user participation through description-writing during image selection produced a retention rate of 95% during the first week for passwords but passive systems achieved only 70%

retention. The analysis establishes that interaction along with personalized choices create strong mechanisms to remember passwords better.

Table 2.3.1 Memory accuracy of different pictures

Image Type	Memory accuracy
Common objects	93%
Abstract Graphics	77%
Natural scenery	85%

The fact that most research has concentrated on the range of four days to one week [3, 5] that indicate that the seven-day is a defining timeframe on assessing the shift of short-term recognition to stable memory retention in graphical authentication.

2.3.2 Cognitive Load and User-Specific Performance

The way users organize and process information during password memorization constitutes an essential factor in memorability performance. Users who displayed a field-independent cognitive style produced better quality graphical passwords that field-dependent users found difficult to remember based on “A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication” [20]. Interface adaptations should modify their complexity settings according to various cognitive abilities of individual users. Security shortcomings arise from linking image choice to memorable episodic events like childhood recollections according to “On Cultural-centered Graphical Passwords: Leveraging on Users' Cultural Experiences for Improving Password Memorability” [21] yet this practice enhances overall memorability. Scientists suggested adopting randomized decoy images for authentication systems because they would help make patterns difficult to detect.

2.3.3 Memorability Challenges and Design Considerations

RGP systems maintain strong characteristics in the face of memorability issues. “An Evaluation Model for Recognition-based Graphical Password Schemes” [22] pointed out password interference as a problem when users fail authentication because they mistake images which appear similar like dog breeds or natural landscapes. A distinctive solution was presented for visual reduction by mixing categories of animals along with landmarks and objects. The evaluation process requires special attention to how the system interface functions for different age groups. The research conducted by “An exploration of graphical password authentication for children” [23] demonstrated that children between ages 6–12 failed to remember abstract pattern designs with a recall rate of under 50% but concrete items such as pizza and soccer balls exceeded 85% of recall success. The data shows that standard pictures benefit users under 18 but suggests that systems designed for this group should maintain accessible understanding and recognizability.

2.4 Recent Literature Review on Recognition-based Graphical Password.

Graphical password schemes based on recognition have been a topic of widespread research in recent years, especially in terms of usability, memorability and security trade-offs. At least ten works that have been published in the recent past have been reviewed in this section with emphasis on their methods, findings, and limitations.

GPOD: An efficient and secure graphical password authentication system by fast object detection [2] : The present paper suggests GPOD, a recognition-based graphical password system, which uses deep learning, specifically, the YOLOv3 object detector algorithm to accelerate authentication and improve security. This system enhances efficiency in the sense that the images are recognized quickly whilst it is resistant to common attacks. Results indicate that the latest AI approaches have the potential to enhance usability and security, and therefore this study is directly applicable to the work that attempts to balance both performance and protection of the graphical password systems.

Graphical Passwords for Emergent Users: A Four-Day Recall Comparative Study on PIN, Passfaces and Celebrities [3] : This experiment compared the usability/memorability of PINs, Passfaces and celebrity-image passwords in the case of emergent users (old-age and novice). Passfaces were more memorable than PINs, but the efficiency of logins was worse over a four-day longitudinal test. The relevancy of the work is that it not only brings out the trade-off between usability and memorability but also offers a model that can be used to perform short-term longitudinal testing.

Deep learning based graphical password authentication approach against shoulder-surfing attacks[8]: This paper presents a scheme based on recognition that takes advantage of deep residual networks (ResNet) with edge detection and image recognition to protect against shoulder-surfing attacks. It is managing the system by a three-stage procedure involving registration, login, and authentication into the system to enhance security and usability. It is also of great relevance to the security assessment of this project because it targets countering one of the most frequent observation attacks.

Graphical passwords: Behind the attainment of goals[9]: This paper critically reviews the research on graphical passwords, and evaluates the trade-offs among the usability, security and memorability of the various schemes. Examples of weaknesses that the authors have explained include shoulder-surfing attack, smudge attack and guessing attack, though the authors have indicated that it is difficult to ensure that the user remains convenient. Being a general survey, it will be useful in contextualizing the given project based on the available research gaps and proving the need to employ balanced design strategies.

Does image grid visualization affect password strength and creation time in graphical authentication? [11]: This experiment looked at the ways in which differences in the visualization of image grids influence password intensity and password-making time. Findings showed that more compact grids resulted in more secure passwords but longer generation time, which points to the usability-security trade-off. The results are highly applicable to the grid-based prototypes in this project in that they give design-based information on the effect of grid layout on the user behavior.

A Preliminary Study to Evaluate Graphical Passwords for Older Adults [13]: This research examined how easily and how memorable graphical password schemes are to older adults who are frequently overlooked as subjects in authentication studies. Findings underscored the need to have simple and intuitive designs to support the cognitive and perceptual constraints. These findings apply to this project because they imply that user-centric design is needed to make accessibility accessible to different populations.

Enhancing graphical password authentication system with deep learning-based arabic digit recognition[14]: In this study, a new graphical password scheme was presented in which users create a sketch of Arabic digits to log in and authenticate with the help of deep learning classifiers. The technique made the technique easier to use with intuitive input, and more secure with digit variation with the support of the Selected Pixels (SP) technique to ensure efficient storage. The emphasis on the implementation of AI into recognition-based schemes shows that niche technologies can enhance functionality and protection, which fits the purpose of balancing usability and security of this project.

A Sector-Based Graphical Password Scheme with Resistance to Login-Recording Attacks [17]: The present paper has suggested a sector-based graphical password scheme, RiS, to be resistant to threats of login-recording like shoulder surfing and video-based observation. It is a system that focuses on flexibility of mobile and touchscreen applications and tries to find a balance between usability and enhanced security. Its specific emphasis on observation resistance applies directly to the context of this project where the issue is to evaluate protection against shoulder-surfing attacks.

A Human-Cognitive perspective of users' password choices in Recognition-Based graphical authentication [20]: This paper examined the effects of cognitive variables, including field dependence and independence, on the choice of images and the recall of those images in the process of creating the graphical passwords using recognition. It was found that users select meaningful or distinctive pictures, which enhance easy recall but at the cost of security because of forecastable patterns. The study points out the usability versus memorability and resistance to guessing attacks trade-off between cognitive ease and password strength, which has direct implications on the scope of this study, namely balancing ease of use and memorability with the resistance to guessing attacks.

'Pictures are easier to remember than spellings!': Designing and evaluating KidsPic — A graphical image-based authentication mechanism [26]: This paper described KidsPic, a graphical password system that can be used with children of age 6 to 11 to supersede the cognitive and usability difficulties associated with alphanumeric passwords. Results revealed that pictures were more memorisable than text, and so the system became more user-friendly with the young audience. The work also presents how age-focused design can be used to increase usability and recollection, which will provide information that is pertinent to the focus of this project balancing memorability with security.

2.5 Gaps and Future Directions in Recognition-Based Graphical Passwords

The analysis of the latest studies of recognition-based graphical passwords identifies the achievements achieved and the issues that exist. Although some schemes prove to be more usable, more memorable, or resist certain attacks, none of them has managed to attain a holistic balance between these aspects. To illustrate the areas where the literature is wanting a bit better, Table 2.5 outlines the key research gaps found in the areas of usability, memorability, security, and overall balance of design. These gaps do not just highlight the shortcomings of current methods but also give some insight into potential future research and development directions.

Table 2.5 Research Gaps in Recognition-Based Graphical Passwords

Dimension	**Identified Gaps**
Usability	The time to perform a log in is frequently longer than a PIN; performance that is not predictable across both prototypes and situations. Not so many studies maximize both speed and accuracy.
Memorability	Most assessments are short-term (days/weeks). There are few studies on longitudinal studies, and long-term retention under actual use is not known.
Security	Observation attack countermeasures are typically tested in controlled laboratory environments; no practical robustness is proved. A great number of solutions compromise usability in favor of increased security.
Design Balance	The usability, memorability, and security of a recognition-based scheme cannot be considered in one single recognition-based scheme. There are still no hybrid methods involving a combination of several aspects of interaction (e.g., dynamic grids with directional input) and systematic multi-dimensional appraisals.

Table 2.5 is the synthesis of the key gaps in research that have been highlighted due to the current studies on recognition-based graphical passwords. The usability is also poor, as the time to log-in may take longer than it takes to use a PIN and is inconsistent between designs. Mostly, memorability is tested over short term, leaving long-term performance under realistic conditions to be unclear. Countermeasures against security attacks in particular on account of observation, are traditionally demonstrated only in the laboratory, and little is known of their usefulness in practice. Finally, there is no current scheme that managed to strike the right balance between usability, memorability and security; hybrid solutions where several techniques of interaction (e.g., dynamic grids with directional input) and multi-dimensional measurements are combined are yet to be established. Such gaps are the driving forces behind the aim of the current project.

2.6 Conclusion of Literature Review

The literature review has indicated that authenticating procedures have evolved and changed their approach to include use of graphical password systems which are meant to exploit human visual capabilities. Even though graphical passwords are easier to use than alphanumeric passwords, previous research indicates that graphical passwords still have significant weaknesses, such as susceptibility to observation attacks, a lack of password diversity, and poor long-term memorability. The use of recognition and recall based mechanisms has been extensively discussed and studies have shown that few systems have been able to incorporate spatial and directional indications to improve in terms of security and usability.

The studies of shoulder-surfing always show that the observed graphical passwords could be reproduced with high precision by attackers, which makes it necessary to develop better countermeasures. Meanwhile, research in cognitive psychology reveals that spatial memory and directional orientation potentially can be of great assistance to long-term memory, promising to improve password retention. But there are few empirical tests linking these mental functions with the password authentication on graphics. Moreover, a significant part of the available literature has been devoted to short-term performance testing, and a rather minor role has been devoted to longitudinal memorability experiments which follow password recall over a long time.

The gaps demonstrated above indicate that a systematic exploration of graphical password systems, which integrate dynamic grid layouts and direction-based authentication systems, is necessary. Specifically, additional analysis is needed to compare their efficiency in registration and efficiency in logging, strength against shoulder-surfing attacks, and durability in their performance in the conditions of daily use. It is through these gaps that the current study will fill in new empirical data that will help further the academic comprehension and the practical design of secure, usable graphical password system.

CHAPTER 3

SYSTEM METHODOLOGY/APPROACH

3.1 Project Development Approach

The development of the gridlock system was done in a systematic and organized fashion and involved the combination of both software engineering principles and empirical research methodologies. Such a two-fold approach made sure that the product was not only a technically sound application, but also a scientifically tested one by means of iterative user testing.

3.1.1 Project Workplan and Task Elaboration

The systematic development of the GridLock authentication system and its timely development required building a systematic project workplan that was strictly followed during the research period of 2026. Instead of using theoretical software development life cycle (SDLC) models, the project was implemented using a more realistic, task-oriented timetable. This method focused on the real technical improvements, testing experiments, and data analysis to reach the established research goals. As shown in Figure 3.x, the project schedule was between February and May 2026 and this involved five major functional stages with strategic overlaps to optimise efficiency.

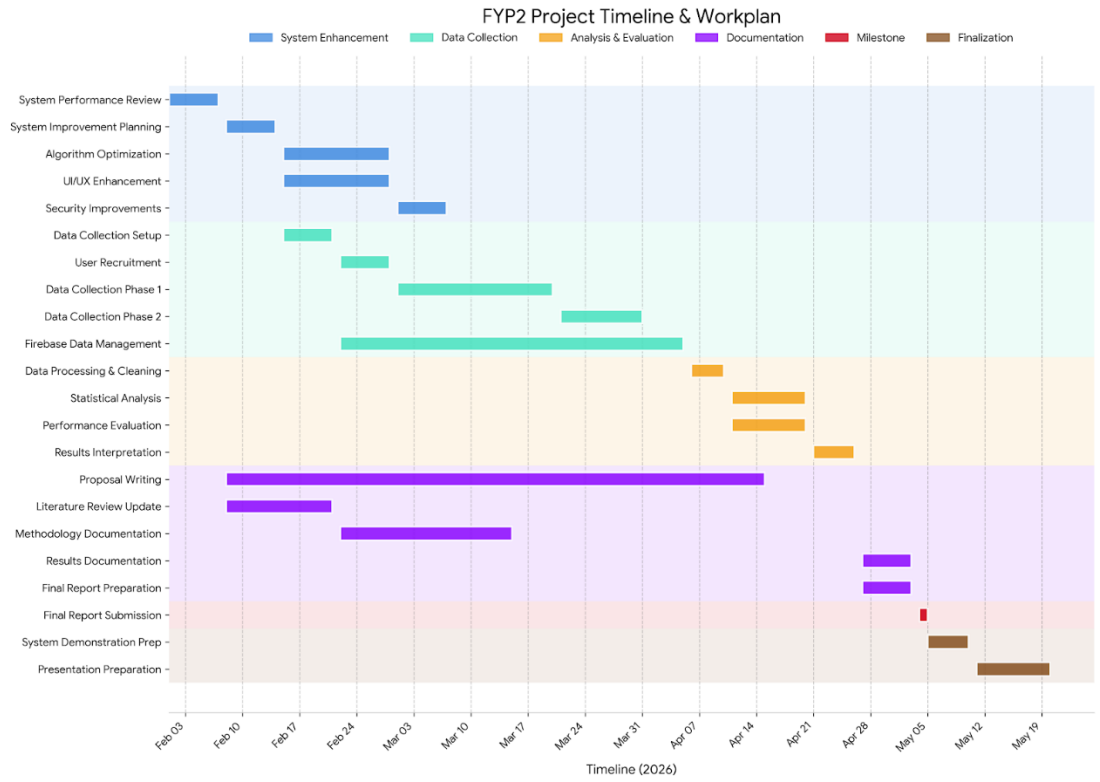


Figure 3.1.1 FYP2 Project Timeline and Workplan

Phase 1 saw the beginning of the project and entailed system enhancement that took place between early February and early March. In this time, a thorough review of the performance of the currently available prototypes of GridLock was conducted to determine and eliminate latency problems. Next, mathematical algorithms of the dynamic compass rotation and edge-wrapping logic were tuned down to ensure spatial accuracy. Meanwhile, the user interface was streamlined to reduce cognitive friction when configuring the passwords, and strong back-end security features were put in place to ensure the integrity of the data when the trials were to occur.

After the first improvements, Phase 2 commenced with the main empirical data gathering between mid-February and early-April. The stage started with the creation of safe testing conditions and the selection of various participants to participate in the longitudinal study. When the participants would use the prototypes in two separate testing stages, the system would automatically measure the most important metrics, such as, the length of login, the success rates, and the number of spatial misclicks. During this time, the Firebase Realtime Database was being administered regularly so

that all the session logs were safely synchronized and properly timed without any information being lost.

After the completion of the data collection, Phase 3 involved analysis and evaluation during the month of April. The raw empirical data that was produced by Firebase were thoroughly processed and cleaned to remove anomalies or partial login attempts. The smoothed data was then analyzed statistically to plot learning curves and identify cognitive plateau levels to make a definite comparison between the two compass models, the static and the dynamic. These results were finally combined to prove the optimum configuration of the 5-object and to demonstrate that the system is absolutely resistant to observation-based attacks.

Concurrent with the technical development was Phase 4, which approached documentation as a continuous, iterative process, between February and early May. The methodology and literature review sections were regularly revised according to the structural changes and emergent theoretical knowledge. During the later weeks, the interpreted analytical data were carefully transcribed into the evaluation chapter of the final report and all the sections were consolidated and formatted in accordance with the official university guidelines.

Lastly, Phase 5 was the completion and handing in of the project deliverables in May. It was a milestone to submit the final copy of the manuscript, including the Turnitin similarity report, on May 4. After the submission, special effort was put into preparing the presentation materials and optimization of the Android application to make the final Viva assessment live product demonstration smooth.

CHAPTER 4

System Design

The implemented system is an Android-based authentication platform that integrates recognition-based graphical passwords with compass-driven directional inputs. The system focuses on three primary factors: effective password generation and entry, resistance to shoulder-surfing and recall when it is reused. The design featured modular features to facilitate the registration of passwords, authentication, experiment management and data collection.

4.1 System Architecture Design

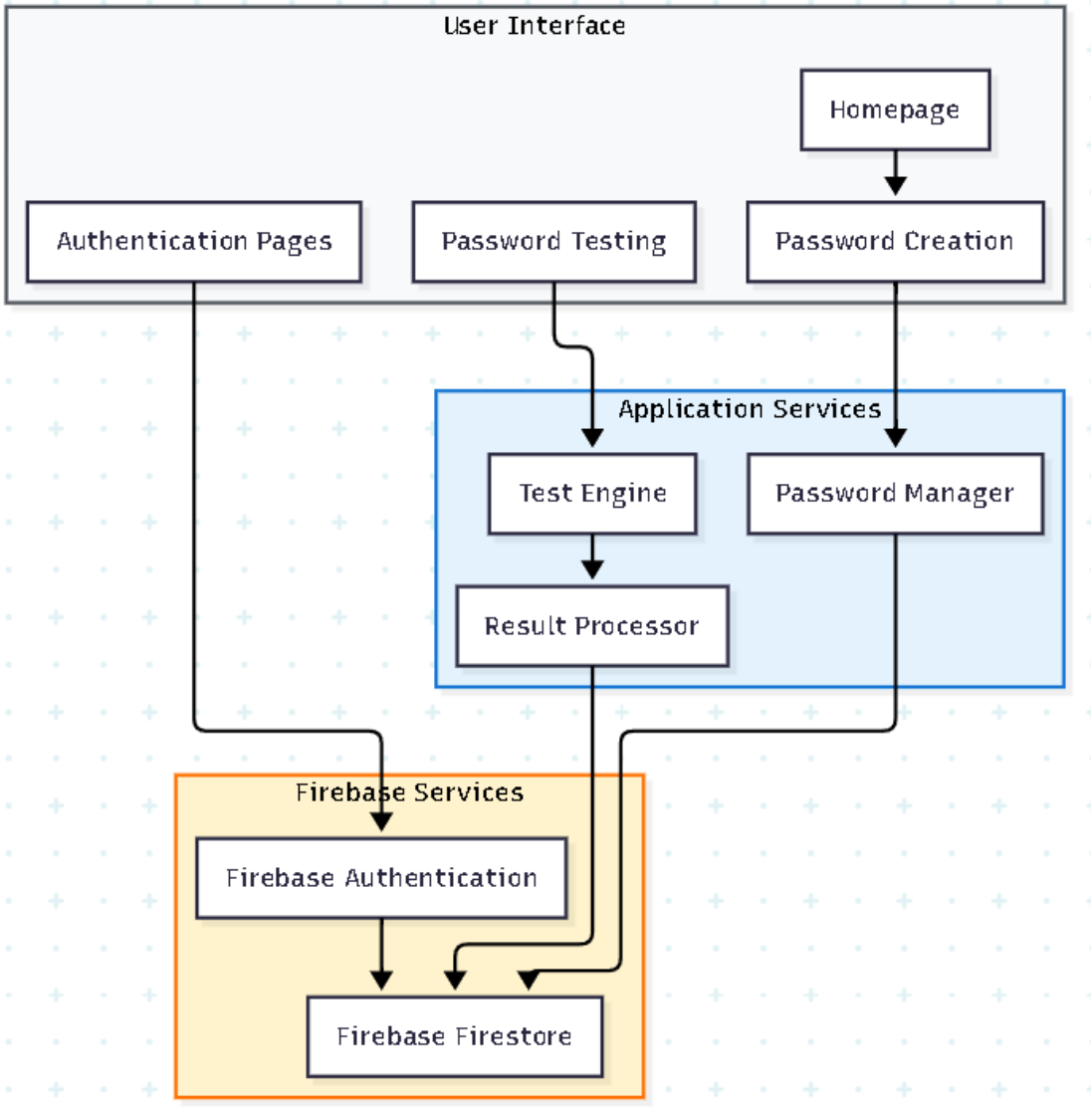


Figure 4.1 System Architecture Diagram

The architecture diagram of the developed graphical password system is illustrated in Figure 4.1. The system architecture comprises of three principal layers, the client-side Android application, application services, and Firebase backend services. In combination, these modules work in integration to facilitate user registration of the user, authentication, password generation, prototype testing, and data storage to facilitate the assessment of usability, memorability, and security.

The Authentication Module act as the front end where a user can create new accounts or log in using the existing credentials. Registration, login, and password reset processes were managed through firebase authentication database. Users are granted access to the application's experimental modules only after successful identity verification. The Homepage serves as the navigation hub. It is here that the user may create new graphical passwords by using the Password Creation module or to the Password Testing module where the user evaluated the previously created prototypes. This structured design ensured seamless navigation and a continuous experimental workflow.

Password Creation enabled the user to create passwords by choosing image sequences and attributing directional inputs. The Password Manager service then processed these inputs, validated the formatting, and synchronized them with the Firebase Firestore. The Password Testing represents a module linked to the Test Engine service, which carries out prototype-specific authentication logic (e.g., Compass Lock or Compass Pro) and verifies user attempts with stored passwords.

Result Processor service is the service which assembles data from testing sessions, such as the time at which it was logged in, the number of errors and success/failure. These metrics were stored in Firestore to create a comprehensive dataset for the comparative analysis of usability and security performance.

Firebase Services provided robust data management at the back end. User accounts were secured using Firebase Authentication, and user profiles, records of passwords, demonstration results, and test outcomes were organized within Cloud Firestore. This integration guaranteed that every user interaction was systematically documented and archived, enabling an empirical evaluation of the system's performance.

The architecture offers technical reliability and research value by decoupling user interaction, application logic and data management. It will facilitate a consistent measurement of the experimental data to explore the trade-offs between usability, memorability and anti-observation attack resistance.

4.1.1 System functionality

The system offered a core functionality to assist users as well as experimental assessment. Users were able to create an account, set passwords based on one of four prototypes (Compass Pro VIII, Compass Pro IV, Compass Lock IV, Compass Lock Pro IV) and log-in to authenticate their identity. To assist the user, there is a tutorial module was included to guide them create and use passwords and a password management module that helps them to view, reset or re-test their passwords that they have stored. Furthermore, the system was designed to demonstrate and test various prototypes and ensure that appropriate data including the registration time, the time of login and the number of errors is always logged to be analysed.

The subsections below outline the operational range and dynamic workflow of the system to define the functional boundaries and logic of human-computer interaction in the system clearly. Instead of being theoretical in nature, this section illustrates the actual user interactions- beginning with the initial account creation and interactive practice demonstrations, all the way to the full performance of the 7-day longitudinal authentication test. The description of these essential functions gives a logical framework on how the technical implementation is to be made and makes the evaluation of the experiment systematic and consistent.

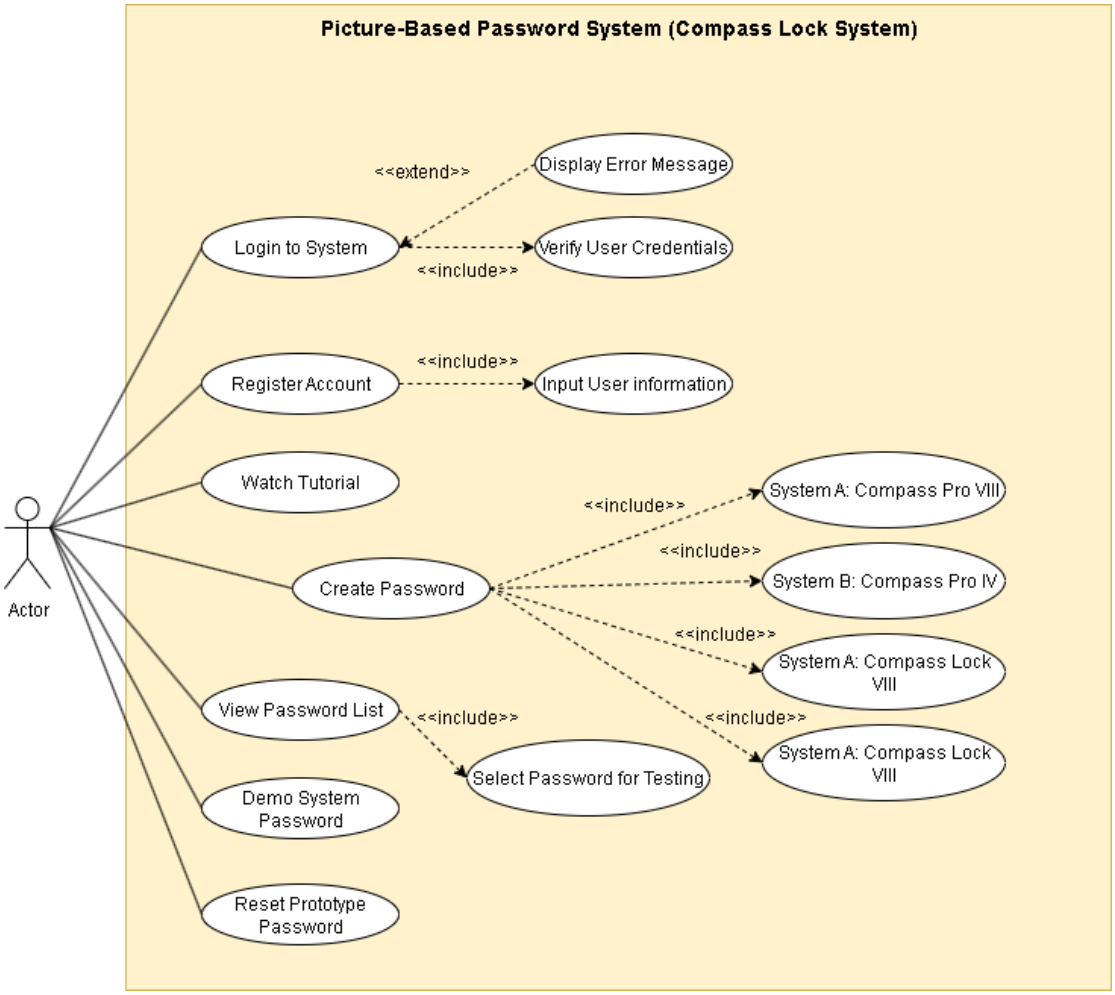


Figure 4.1.1 System Functional of the gridlock System

As illustrated in Figure 4.1.1, the system functional model provides a high-level visual interpretation of the functionalities of the GridLock system. It demonstrates the interaction between the external actor (the test participant) and the core processes of the system. The architecture revolves around a single primary actor, since the GridLock system is constructed specifically as an experimental testbed for graphical authentication and usability evaluation.

4.1.1.1 Participant Interaction Scope

The User or Participant is the only external agent that interacts with the GridLock system. This actor is a symbol of the participants of the longitudinal usability and security study. Their main duties include creating an account, setting their spatial-directional graphical password, going through the onboarding demo, and making daily authentication attempts with the purpose of producing the required empirical test data.

4.1.1.2 Core System Operations

The system has five main use cases that control the interaction of the user during initial onboarding, up to daily testing.

Register Account, which enables a new participant to generate a test profile, is the first core use case. If the user does not already have an active account, the user enters the landing page of the system and provides a unique identifier, like a Participant ID. This input is validated by the system to eliminate duplications and then the account is successfully generated, and the profile is safely stored in the database, and the user is redirected to the configuration phase.

After registering an account, the user goes to the Complete **Demo Phase** (Onboarding). This interactive guide has been clearly created to assist users to overcome the initial cognitive resistance and learn the authentication process before establishing their own credentials. The system gives visual clues and, in the case of dynamic prototypes, details the operation of the randomized indicator of North. The participants undergo practice authentication trials with a predetermined sequence and get real-time feedback (success or failure) until they internalize the underlying mental rotation logic.

After the Demo Phase, there is the **Configure Graphical Password** use case that enables the participant to specify his/her own authentication credentials. The user then decides on the complexity of the password they would like to use (e.g., 4, 5 or 6 objects) and is presented with a grid of the possible visual object pool. The participant chooses target objects in a particular sequence based on their assigned prototype (Systems A, B, C, or D) and assigns a spatial direction to each object. Once the user confirms the final sequence, the system then safely encrypts and records such pairs of Object + Direction to the account, which prepares the participant to undergo official daily testing.

Perform Authentication (Login) use case summarizes the essence of the empirical study. In this daily operation, the system produces an authentication grid containing randomly shuffled visual objects and in the case of dynamic systems, a newly produced orientation of North. The participant does a visual search to find their objects as targets and carries out mental rotation to compute the appropriate grid cells depending on the memorized directions. They successively mouse over these calculated cells and the system compares the spatial-directional information to the database. A successful validation will allow access, whereas a wrong sequence or a wrong click will cause a denied attempt. In both cases, the system carefully records session measurements, such as the time of the first login and the accuracy, which are the main data that can be analysed by the Human-Computer Interaction (HCI) in the future.

Lastly, the **View Test Results** use case enables participants to track their personal performance. Once authenticated into the system, users have access to a personal dashboard where the system retrieves their past logs of logging into the system. The interface then shows a combination of performance data, including their average history of time to log in and their general success rate during the longitudinal study.

4.1.2 System Workflows

Based on the basic system operations developed in the preceding section, there was a need to map the dynamic behaviour and operational processes of the GridLock system. This part describes the chronological rationality, choice components and pathways that study participants followed. Describing such operational workflows, the inner logic of the system is explained, especially how the first-user onboarding step was smoothly transitioned to the realization of the spatial-directional authentication process.

4.1.2 1 User Login and Registration Process

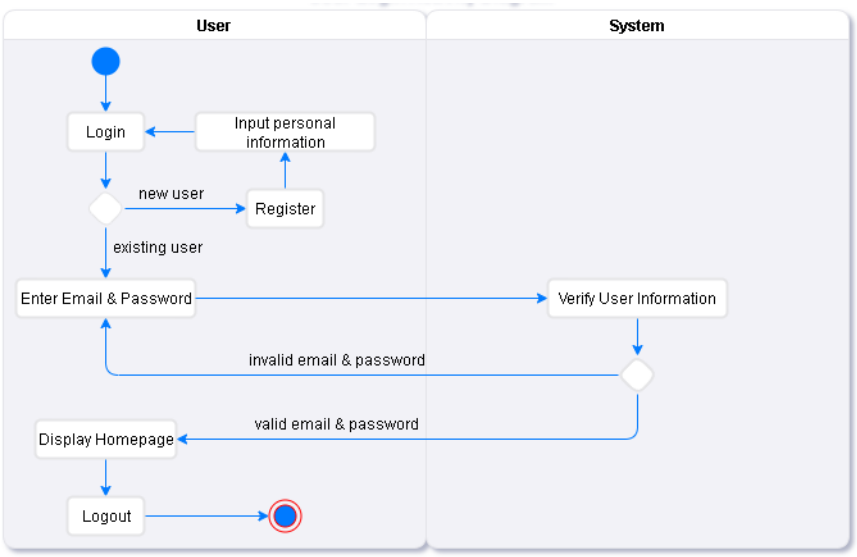


Figure 4.1.2.1 User Login and Registration Process

Figure 4.1.2 1 illustrates the system access workflow. New users created an account, whereas older users accessed the system using previously stored credentials. The system validated the entries and gives entry to the homepage or causes correction of the error.

4.1.2.2 Password Configuration and Reset Flow

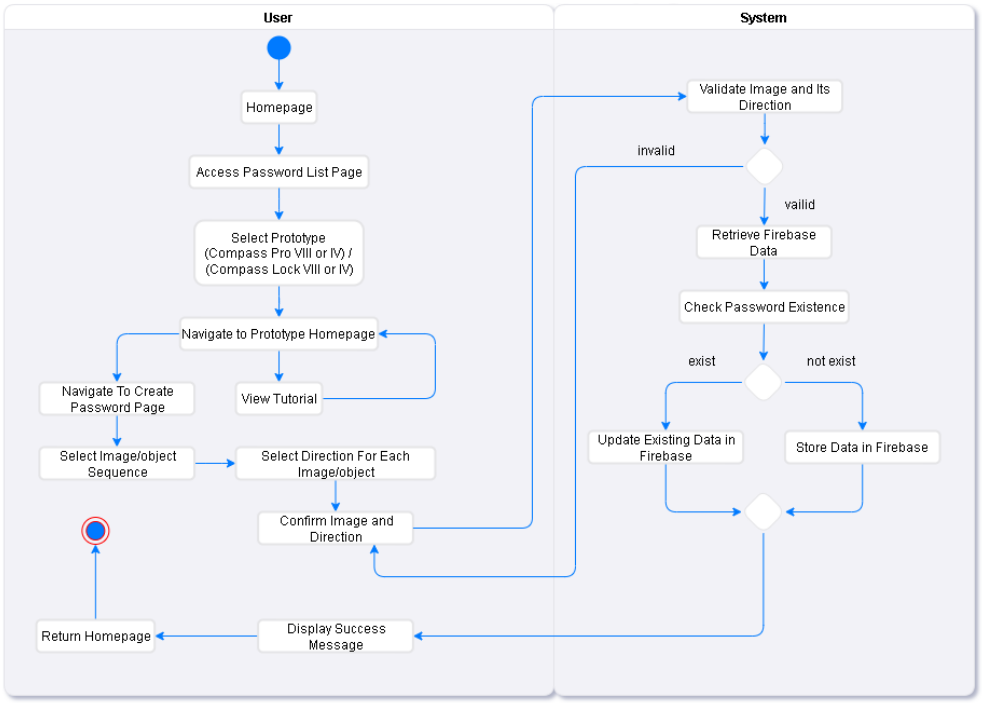


Figure 4.1.2.2 Password Configuration and Reset Flow

As depicted in Figure 4.1.2.2 the password creation process involved choosing an image sequence, providing directional inputs, and validating the final order. The system authenticated the configuration and synchronized the data with Firebase. There is a reset button was implemented that makes it possible to reconfigure without having to create a new account.

4.1.2.3 User Demo Prototype Password Process

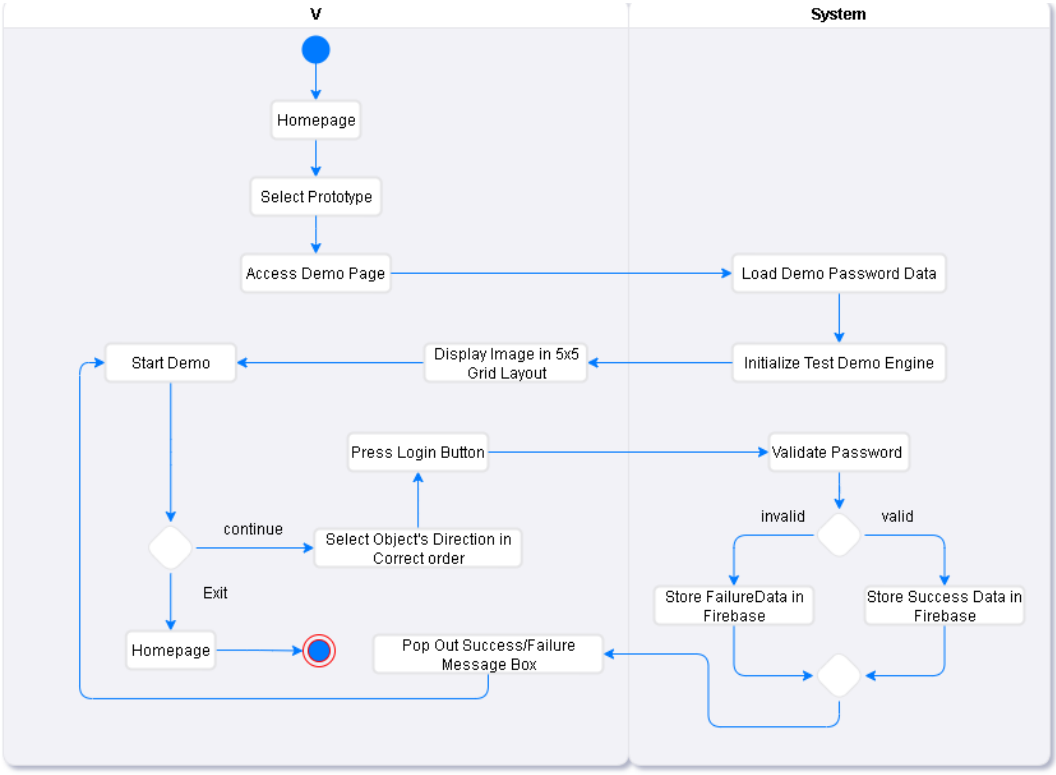


Figure 4.1.2.3 User Demo Prototype Password Flow

Figure 4.1.2.3 represents the demonstration mode designed for user practice. In this flow, users were guided through a demonstration password sequence where they selected images and directions and received immediate feedback. This module enabled users to repeat the demo or proceed to the homepage once they became familiar with the mechanism

4.1.2.4 User Test Compass Lock VIII or IV Process

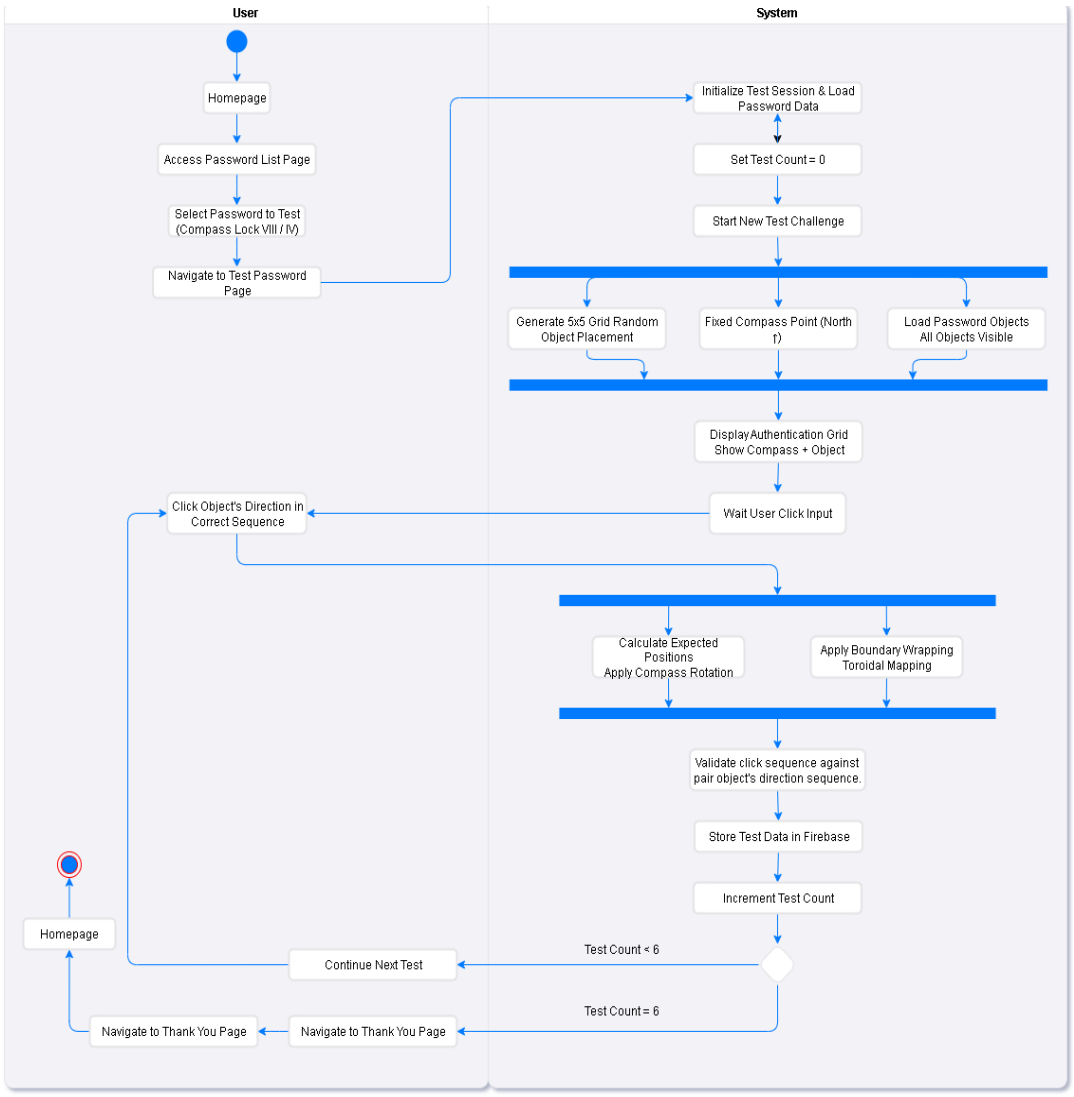


Figure 4.1.2.4 User Test Compass Lock VIII or IV Flow

Figure 4.1.2.4 details the evaluation procedure for the Compass Lock IV and VIII prototypes. Users selected their saved credentials from the password list module and performed six login attempts and the system tracked and recorded the login time, failures count, and success rate.

4.1.2.5 User Test Compass Pro VIII or IV Process

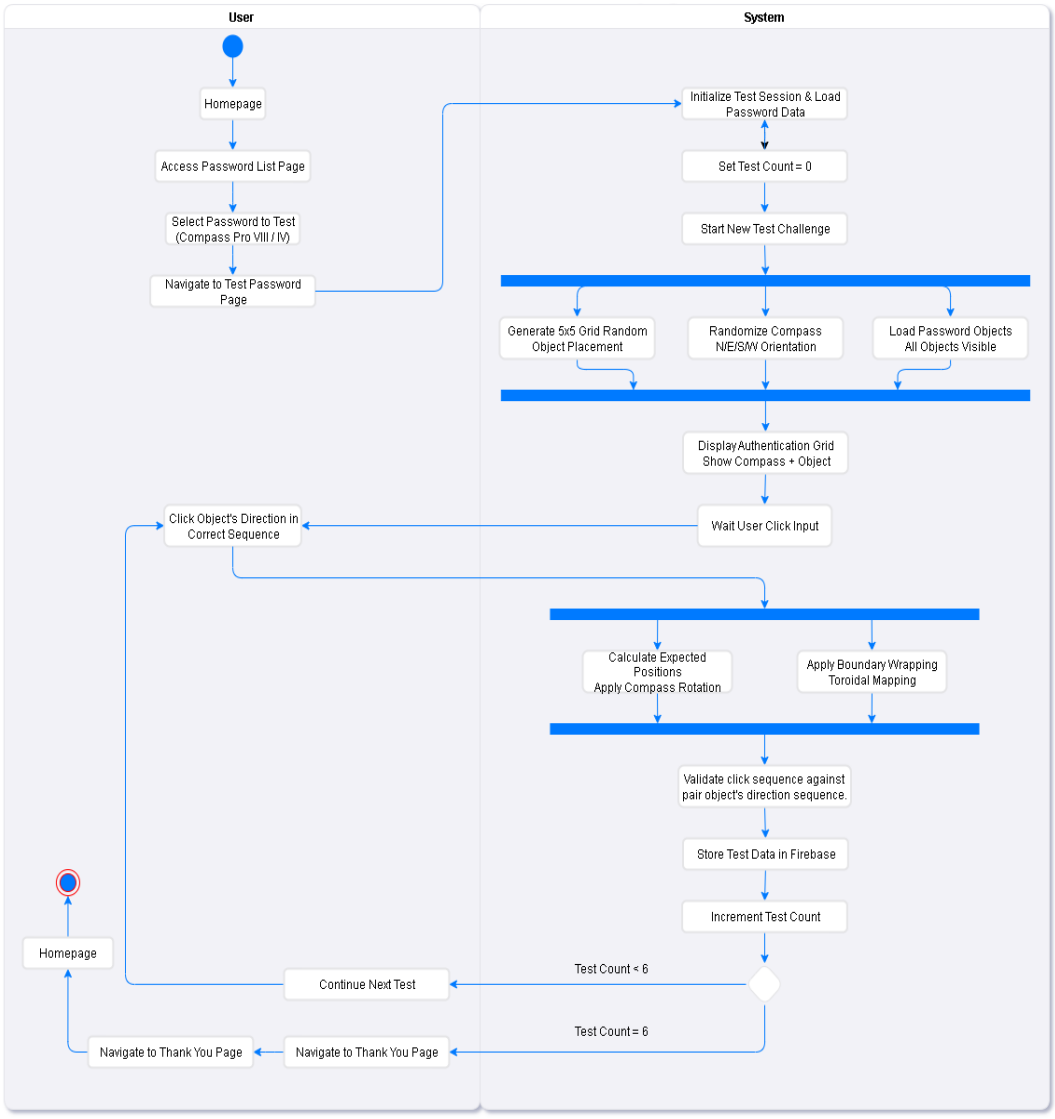


Figure 4.1.2.5 User Test Compass Pro VIII or IV Flow

Figure 4.1.2.5 demonstrates the testing procedure of the Compass Pro prototypes. Users choose their password that is saved, and it tries to log in six attempts under dynamically changing compass positions. The system documented the resulting performance metrics to facilitate a detailed analysis of the dynamic randomization's impact on usability.

4.2 Authentication Logic and Prototype Variations

The authentication scheme that was put in place was tailored to critically analyze how the dynamics of the compass and the complexity of directions affect user performance. In an attempt to have a complete account of the trade-offs among the usability, security, and memorability, the system structure was developed based on a standardized grid framework, on which four different prototype versions were implemented.

4.2.1 Core Authentication Mechanisms and Grid Logic

The basic authentication code was the same throughout the system, irrespective of the prototype under test. The interface was based on a grid system (5x5) in which visual objects were randomly assigned a location per session to prevent a simple pattern memorization and observation attack, so that the location in space was varied. The only way an authentication attempt was considered successful was when the user selected the correct target objects sequentially and used the exact memorized directional mapping on each.

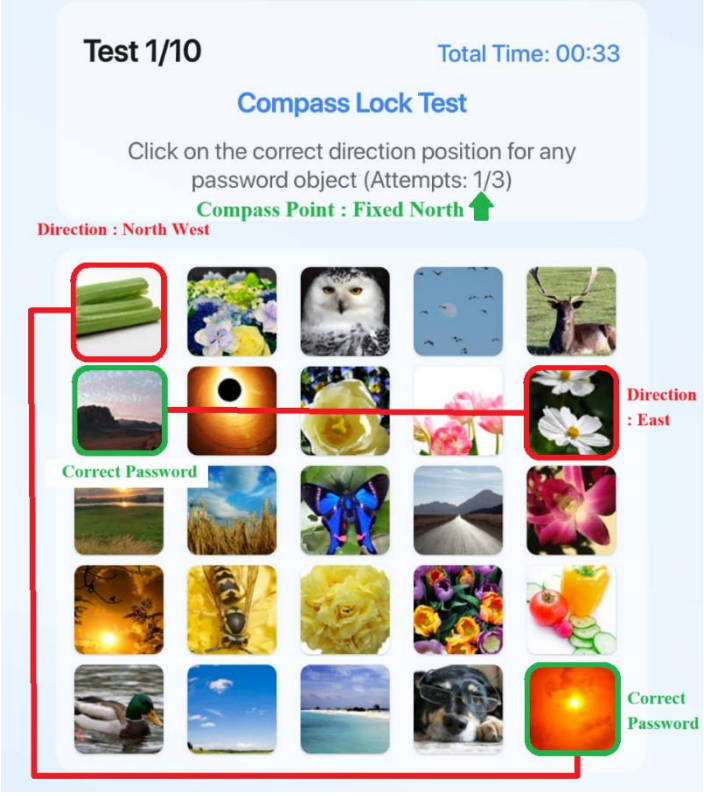


Figure 4.2.1 Edge Wrapping Algorithm for grid boundary navigation

Most importantly to make sure the experience of interaction is smooth throughout the interface, an Edge Wrapping Algorithm was standardized throughout all prototypes. This algorithm (as shown in Figure 4.2.1) handled directional inputs at grid boundaries. An example is that when a user took the object located in the top row and passed a directional input of North, the algorithm dynamically repositioned the choice to the cell located at the lower part of the identical column. This homogeneous logic of boundary was such that users could deal with edge or corner objects without functional discontinuities. Moreover, the system included a single- click validation system to verify in real time the spatial verification as well as an attempt-restriction protocol to counter the vulnerability of brute force.

4.2.2 Prototype Variations and Complexity Trade-offs

The implemented authentication framework utilized four prototype models designed to critically examine the impact of compass dynamics and directional complexity on user performance. All the models were defined by a particular combination of behaviours of the compass (dynamic vs. static) and directional granularity (8-direction vs. 4-direction) and allowing for a comprehensive evaluation of the trade-offs between usability, security, and memorability.

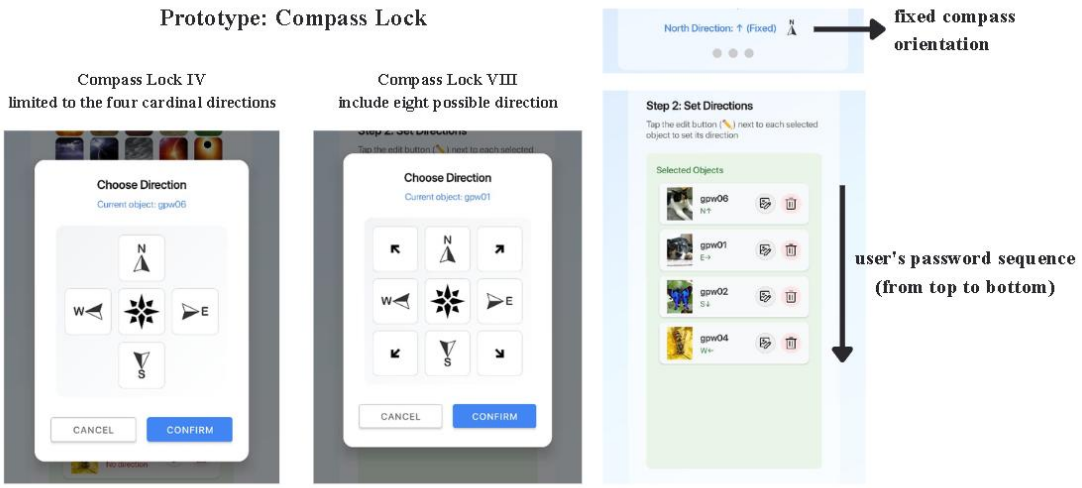


Figure4.2.2.1 Compass Lock Authentication

Compass Lock IV (Static, 4 Directions): This is a base model as depicted in Figure 4.2.2.1 at the upper-left corner and used a fixed compass direction where the North direction was always upwards. The directions were restricted to four cardinal directions (North, South, East, West). Since the mapping was spatially consistent in all logins, this model provided the most efficient performance and minimum cognitive load due to high dependence on muscle memory. Nonetheless, it offered the least password space and variability with the ability of potential observers.

Compass Lock VIII (Static, 8 Directions): As demonstrated in the top-right quadrant of Figure 4.2.2.1, this model did not give up the fixed compass direction (fixed North), but finer-grained it to create eight potential vectors (the addition of Northeast, Southeast, Southwest, and Northwest). When a password was defined as Cat-Northeast, Car-West, Tree-South the spatial mapping was the same when authenticating. This architecture enhanced the entropy of the passwords generated over the baseline model yet maintaining the experience of fast login, just that it was still susceptible to sophisticated shoulder-surfing since it could be identified as a static target..

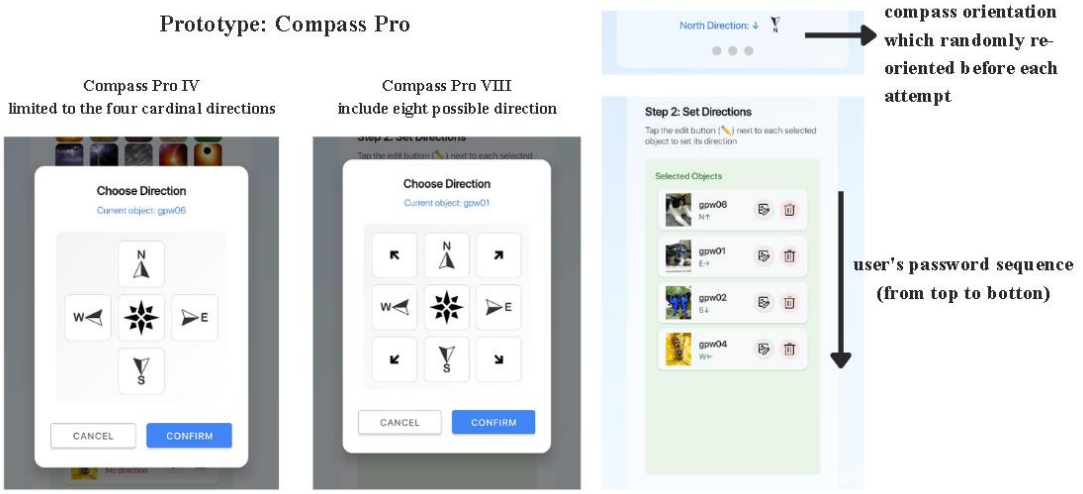


Figure 4.2.2.2 Compass Pro Authentication

Compass Pro IV (Dynamic, 4 Directions): This prototype, presented in the bottom-left section of Figure 4.2.2.2, was the first prototype to add dynamic complexity by randomly resetting the compass before each attempt to log in (e.g. the North indicator would be facing to the right). Although they could only choose directional options within four cardinal directions, users had to rotate their spatial mapping mentally to fit the new compass setup. This dynamic mechanism helped greatly to increase security as the input logic was less readable to observers, providing a reasonable trade-off between application efficiency and high password entropy.

Compass Pro VIII (Dynamic, 8 Directions): This model, illustrated in the bottom-right quadrant of Figure 4.2.2.2, was the most complex model with both dynamic rotation of the compass and 8 directional granularities. At the login stage, the user was required to process a randomised compass orientation and use an 8-directional mapping. Although this mechanism provided maximum password entropy and the greatest theoretical resistance to observation attacks, it required the greatest cognitive load in the authentication process.

Regardless of the model, an authentication attempt was successful only when the selected image sequence matched the stored directional values. These four designs facilitated a systematic analysis of the trade-offs between usability, memorability, and resistance to shoulder-surfing attacks by providing a spectrum of complexity and randomization.

4.2.3 Compass Lock IV Authentication Workflow

To provide a comprehensive understanding of the user interaction and the sequential logic of the GridLock system, the following sections detail the step-by-step authentication process of a user with a four-object password sequence. This scenario is based on the final version of the Compass Lock test interface shown in Figure 4.2.5.

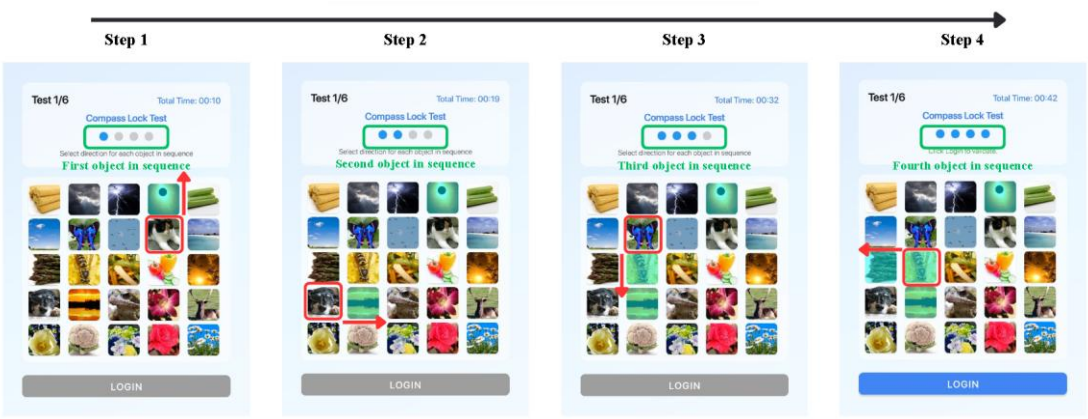


Figure 4.2.3 Compass Lock IV Authentication Workflow

In this case, Consider the user of the following credential sequence stored in the system:

1. Object: "Cat" → Direction: North (N)
2. Object: "Dog" → Direction: East (E)
3. Object: "Butterfly" → Direction: West (W)
4. Object: "Bee" → Direction: South (S)

There are four consecutive steps in the process of authentication, followed as follows: In the initial step, the lead object should be identified via a visual search (Figure 4.2.3). The shuffled image authentication grid is shown as explained in the first panel of Figure 4.x that shows that the labels are Step 1. The top bar (highlighted by a green circle) will show the user that he is dealing with the first object in the sequence. The stored primary target of the user in this case is the image of the cat. The subject will have to conduct a visual search to find this image at randomized grid (marked by the red square). After the Cat identification, the user opens the input by clicking on the cell over the target (denoted by a red arrow) which would be the memorized directional pairing of North. This step initiates an ongoing process of Data Recording in the background.

Step 2: Processing the Second Credential (Figure 4.2.3). After an effective input in Step 1, the interface will update flawlessly. Figure 4.2.3 with the progress bar on the “Step 2” panel now indicates the second dot. The system automatically switches to anticipate the spatial input of the second object in the sequence. After finding the stored image of a dog in the grid (marked with a red square), the user needs to run the given input of East. Because the grid layout followed by the gridlock system is standard, the East is a click of the cell which is physically on the right side of the target image (pointed out by the red arrow). The system automatically manages the wrapping logic if the object is on the grid's edge and continues data recording.

Step 3: Sequential validation of the Third Object (Figure 4.2.3). This is followed by the next panel of Figure 4.2.5 which is the "Step 3" panel. The progress bar has also shown that the user is dealing with the third object in the order. The participant has rightly recognized the Butterfly image (marked by the red square) among the rest of the distractor images. After their memorized combination, they perform the input by clicking the cell that is at the physical left of the target (indicated by the red arrow), the cell that is the "West directional pairing”. The boundary logic in the system as described in Section 4.2.1 makes sure that this input is faithfulness that will in fact be registered even when the object is at the Western edge of the grid which makes sure that a functional discontinuity is not involved.

Final validation and submission (Figure 4.2.3) This step should cover the last verification and submission. Figure 4.2.3 shows the last step in the panels of "Step 4". The progress bar now marks all four dots, and this is because the user is processing the fourth and final object in sequence now. Once the target (the picture of a bee) has been found in the grid (marked with the red square), the subject of the experiment makes the completion of the sequence and does the memorized input (to execute the input of a bee). This will include clicking the cell in the grid that is currently underneath the target object (referred to by the red arrow). Once all four objects have been spatially-directionally validated, the "Data Recording" process is finished, and the primary "LOGIN" button in the bottom of the interface alters its visual state (e.g., turns blue like in Panel 4). This participant is now allowed to press this finalized button to submit his or her full sequence to the final server-side validation mechanism.

4.2.4 Compass Lock VIII Authentication Workflow

To give a detailed explanation of the user interaction and the sequential logic of 8-way directional granularity, the next section explains the step-by-step authentication process of the prototype of the Compass Lock VIII. This situation, shown in Figure 4.x, shows how the participant performs a sequence of four objects using cardinal and ordinal (diagonal) directions with the constant orientations of the compass.

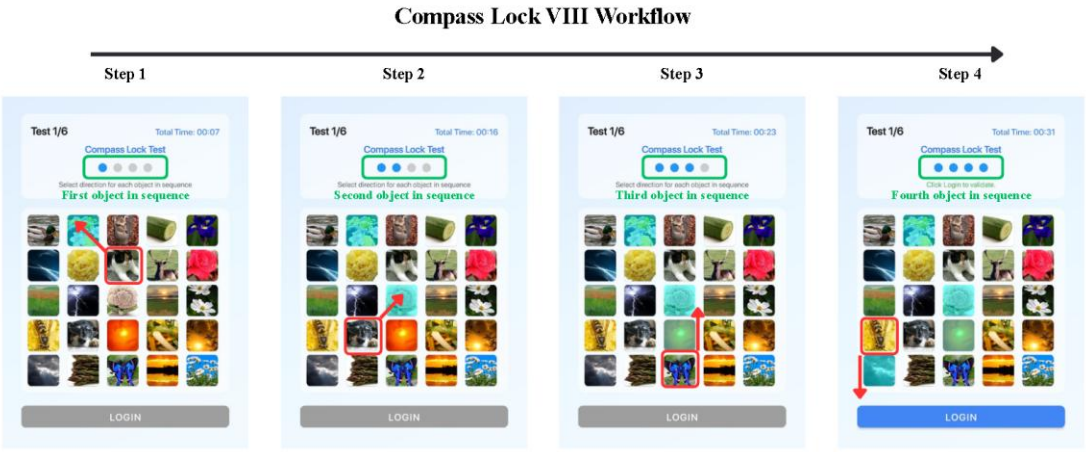


Figure 4.2.4 Compass Lock VIII Authentication Workflow

In this case, Consider the user of the following credential sequence stored in the system:

1. Primary Object: "Cat" → Direction: Northwest (NW)
2. Second Object: "Dog" → Direction: Northeast (NE)
3. Third Object: "Butterfly" → Direction: North (N)
4. Final Object: "Bee" → Direction: South (S)

As shown in Figure 4.2.4, the first step is Diagonal Execution of the Lead Object. The authentication session starts with a randomized grid, 5x5 as shown in the first panel. The top progress bar (circled in green) shows the system is waiting to receive the input of the first object in the sequence. The visual search is conducted by the participants in order to find their main interest, the "Cat" (marked by the red square). On identifying, the user recalls the memorized directional pairing of the Northwest. As the Compass Lock VIII has a fixed North at the top, the user completes the input process by selecting the cell in the diagonally right top of the target image (marked with the red arrow).

As shown in Figure 4.2.4, the second step involves processing the Second Ordinal Direction. After the first input has been successful, the interface is dynamically updated, moving the progress bar to the second position. The second stored image, the "Dog" is scanned by the user on the grid. This object is assigned to the direction of " Northern East". With the help of the 8-directional logic being at rest, the participant chooses the grid cell that is located diagonally to the upper-right corner of the Dog (marked with the red arrow). This ordinal coordinate is documented by the system, and it goes to the next stage.

The third step is pointed out by the progress bar in the third panel. The user recognizes image Butterfly in the grid. In the case of this object, the credential uses a standard cardinal direction: "North" one. The subject performs spatial mapping by clicking the cell just over the target object (highlighted by the red arrow). This illustrates the capability of the system to smoothly combine both diagonal and straight vectors in the same sequence of passwords, which substantially enhances the possible password entropy.

As shown in Figure 4.2.4, the last step is to make the user process the fourth object. Progress bar indicates that the sequence is almost complete. The user finds the image of the bee and utilizes the last memorized direction, which in this case is the South and then clicks on the cell right below the target (the red arrow). When this last spatial input is registered, the system validates the entire 4-object sequence on a local basis. The main "LOGIN" button changes the disabled grey state to the active blue state as the visual feedback. The participant will end the session by clicking on this button, which will initiate the last server-side authentication request.

4.2.5 Compass Pro IV Authentication Workflow

To illustrate the dynamic behaviour of the system and the cognitive loads that the system imposes on the user, the next section will elaborate on the authentication process of the prototype of the compass pro IV. This prototype, in contrast to the statical models, requires a spatial transformation in mind. Figure 4.2.5 shows a full four-object login session in which the system has randomly rotated the compass before the attempt.

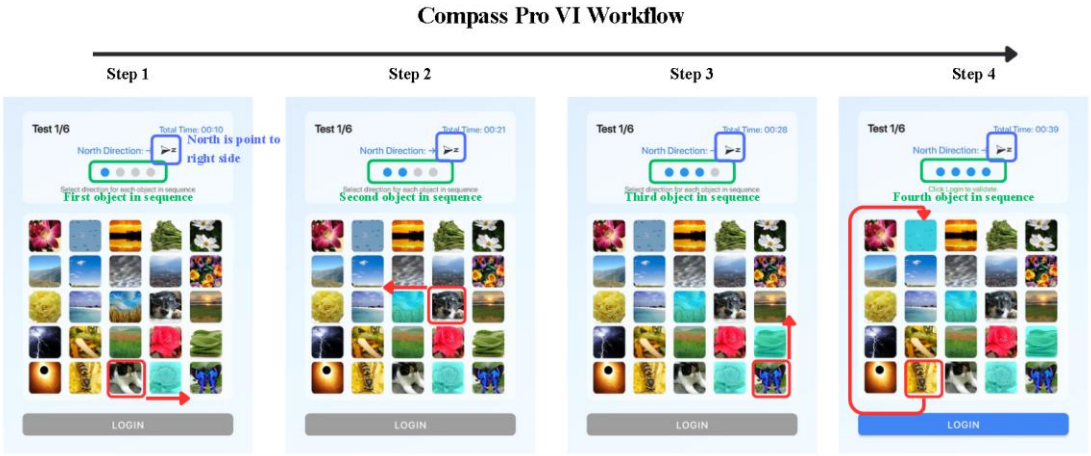


Figure 4.2.5 Compass Pro IV Authentication Workflow

This login session has caused the system to randomly turn the compass 90 clockwise as shown in the blue box of all panels in Figure 4.2.5. As such, the logical North indicator now points into the physical right side of the screen. To bring their entire directional mapping to conform to this new reality, the user must mentally spin around his entire directional mapping. In this case, Consider the user of the following credential sequence stored in the system:

1. Primary Object: "Cat" → Direction: North (N)
2. Second Object: "Dog" → Direction: South (S)
3. Third Object: "Butterfly" → Direction: West (W)
4. Final Object: "Bee" → Direction: East (E)

.

As shown in Figure 4.2.5, the first step is mental remapping for the lead object. The sequence is initiated when the user searches the main target, the "Cat". A directional input of a North is determined by the memorized password. But due to the compass showing that logical North is now to the physical right, the user will have to override his or her fixed muscle memory. The participant effectively maps the mental map and performs the input by clicking on the cell towards the physical right of the target image as shown by the red arrow.

As shown in Figure 4.2.5, second step is inverse Spatial Calculation. Moving on to the second item, the user finds the "Dog". The stored direction is "South. After realizing that South is diametrically opposite to North and that currently the North is at the right, the user works out logical South is now at the physical left. This spatial calculation is performed by the user clicking the cell which is directly left of the Dog image (marked with the red arrow).

In third step, the input required to use the third object, the Butterfly, is West. Physically, West is left in a typical arrangement. But with the present 90 clockwise rotation the logical West axis has moved to the physical top of the grid. When the Butterfly is found, the user can do this orthogonal transformation correctly by picking the cell that is directly above the target (marked with a red arrow).

As shown in figure 4.2.5, edge wrapping execution is the fourth step. The last item, the "Bee" offers a special functional situation. The direction that is memorised is the East, which, in the current rotation, is the physical bottom of the grid (the opposite of the West). The target "Bee" image is found on the absolute bottom edge of the grid. The system will activate the Edge Wrapping Algorithm when the user uses the downward input. The input perfectly wound around the boundary, indicating the selection in the very top cell of the same column, which is explicitly traced by the long red arrow in Panel 4. When this last validation is successful, the main "LOGIN" button triggers and the dynamic authentication cycle is complete.

4.2.6 Compass Pro VIII Authentication Workflow

To illustrate the pinnacle of cognitive complexity and security within the GridLock framework, the following section details the authentication workflow for the Compass Pro VIII prototype. This model merges 8-way directional granularity with a dynamic, randomized compass orientation. Figure 4.2.6 demonstrates a complete login session where the user executes complex ordinal (diagonal) inputs under a severe rotational shift, heavily utilizing the system's edge wrapping algorithm.

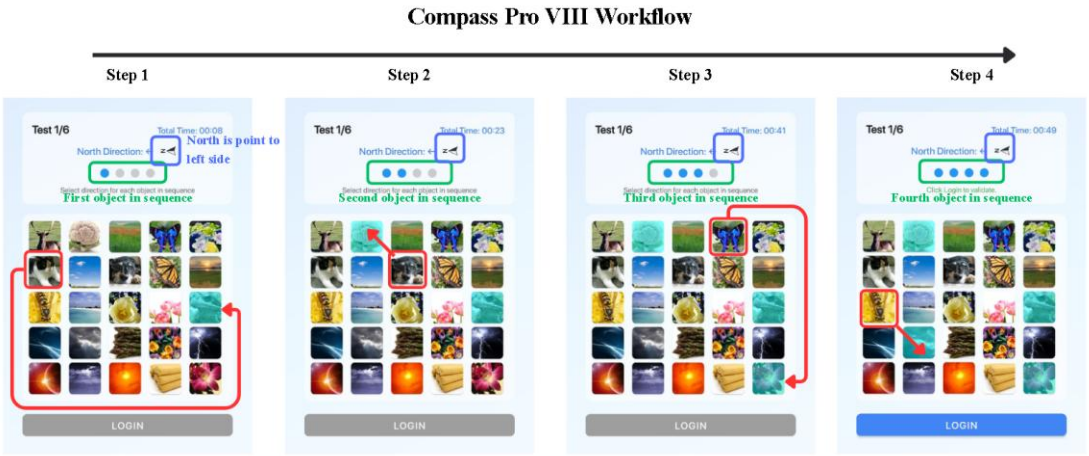


Figure 4.2.6 Compass Pro VIII Authentication Workflow

As explicitly highlighted by the compass indicator across all panels in Figure 4.2.6, the system has randomly rotated the logical "North" 90 degrees anticlockwise for this session. Consequently, the "North" indicator now points to the physical left side of the screen. This forces a complete mental recalibration of the 8-way axis: if North is physical Left, then East is Up, South is Right, and West is Down. In this case, Consider the user of the following credential sequence stored in the system:

1. Primary Object: "Cat" → Direction: Northwest (NW)
2. Second Object: "Dog" → Direction: Northeast (NE)
3. Third Object: "Butterfly" → Southeast (SE)
4. Final Object: "Bee" → Direction: Southwest (SW)

As shown in figure 4.2.6, first step is diagonal remapping and edge wrapping. The user locates the "Cat". The memorized direction is "Northwest" (NW). Based on the mentally rotated axis (North=Left, West=Down), the logical NW vector translates to the physical bottom-left diagonal. However, the Cat is situated on the absolute left boundary of the grid. Attempting to execute a "left and down" input triggers the system's edge wrapping algorithm. As shown by the red arrow in Figure 4.2.6 panel 1, the horizontal component of the input wraps across the grid, successfully registering the cell on the far physical right, one row down.

The second step is ordinal spatial calculation. As shown in figure 4.2.6, the user identifies the "Dog" and stored direction is "Northeast" (NE). Applying the rotated mental model (North=Left, East=Up), the logical NE vector corresponds to the physical top-left diagonal. The user performs this ordinal spatial calculation and executes the input by selecting the cell located diagonally to the top-left of the Dog image (indicated by the red arrow).

As shown in figure 4.2.6, third step is complex vertical Edge wrapping. The user spots the "Butterfly" positioned on the top edge of the grid. The required direction is "Southeast" (SE). Under the current rotation (South=Right, East=Up), the SE vector translates to the physical top-right diagonally. Because the target resides on the uppermost boundary, applying an "upward" vector invokes the vertical edge wrapping mechanism. As illustrated by the sweeping red arrow in Figure 4.2.6 Panel 3, the vertical input wraps around to the absolute bottom row while simultaneously shifting one column to the right, flawlessly executing the complex diagonal boundary mapping.

For the final object, the "Bee", the memorized direction is "Southwest" (SW). Recalibrating to the rotated compass (South=Right, West=Down), the logical SW vector corresponds to the physical bottom-right diagonal. The user executes this final spatial transformation by clicking the cell diagonally to the bottom-right of the target. Upon successful validation of this cognitively demanding sequence, the primary "LOGIN" button activates, allowing the user to finalize the authentication process.

4.3 Database Architecture and Entity Relationships

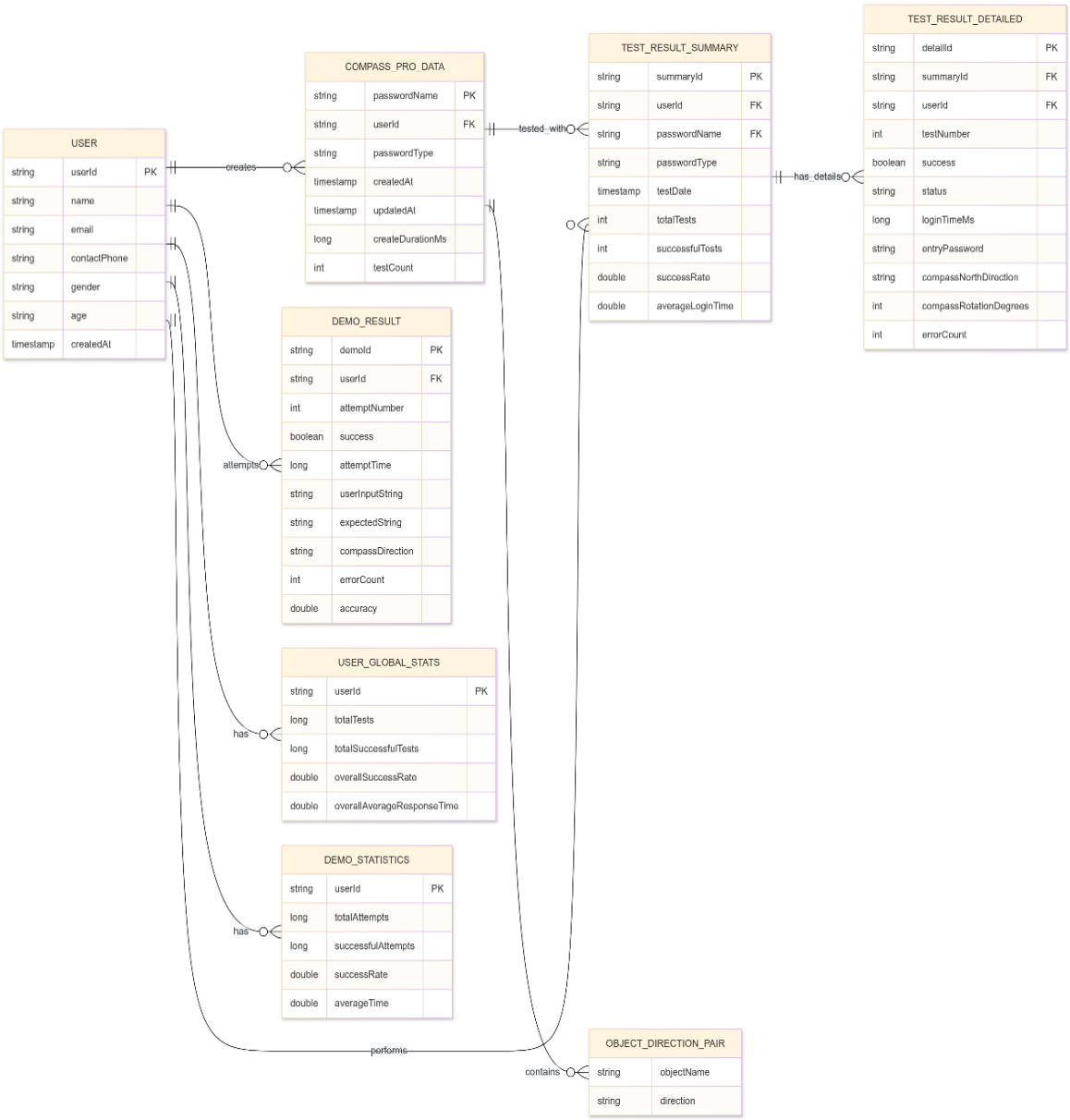


Figure 4.3 Entity-Relationship Diagram (ERD) of the GridLock database architecture.

Google Cloud Firestore represented a NoSQL document database that was employed in this project that helped to organize and manage authentication data and the results of the experiment in an efficient manner. The database structure has multiple collections to take the important entities into the system.

The User collection stored essential attributes, including user ID, email address, demographic, and the time the user was created. This enabled the identification and safe handling of the data of every participant. The Compass Pro Data collection documented the created graphical passwords of the participants, such as the type of prototypes used (e.g., Compass Pro VIII or Compass Lock IV), password name, time stamp, and list of image-direction pairs used to construct the sequence. These stored records were systematically correlated with authentication attempts to validate them.

The TestResults collection tracked the information concerning login and a testing session. Attributes like user ID, password ID, prototype type, time of login, the number of errors, and successful or unsuccessful result are included in each record. This featured form the basis of the data used in testing usability, memorability and security performance. DemoResults collection archived the result of demonstration runs, such as, did users manage to complete the series of passwords generated by the system, the time taken to complete the demo, and how many errors users made during the demo.

Such collections were linked to one another with logical relationships, which provides data integrity and consistency. A user may have one password or many passwords with a password assigned to a single user. In the same way, there are numerous test results related to each password, although there is only one test result related to a single password. Demo results were also correlated to prototypes but were maintained separately to user-created test data to distinguish between learning opportunities and formal tests. This framework guaranteed that the performance of authentication can be traced to participating individuals and to definite prototypes, and it could be analyzed systematically, in terms of usability, memorability, and attack of observation resistance.

CHAPTER 5

System Implementation

5.1 Hardware and Software Setup

For developing and analysing the GridLock framework, there was some amount of hardware and software requirement for ensuring a smooth integration between the Android mobile application and the cloud server.

The selected hardware provided necessary computational power for the Android application compilation and execution process, a trouble-free experience of working with Android Studio integrated development environment (IDE) and adequate processing capabilities to support the work with emulators, database queries, and experimental data processing. The onboard compatibility with a discrete graphics card ensured high responsiveness during heavy rendering workload.

This software platform consisted of tools essential for creating and testing the graphical prototypes on Android-based graphical passwords. Android Studio gives a powerful IDE for code editing, user interface designing and emulator-based testing platform, while Java and XML were employed to implement the program logic and dynamic user interface display. The backend service of Firebase is used to synchronize data in Realtime, securely authentication, and on-demand experiment data storage in the cloud.

Table 5.1 Specifications of laptop and Software environments

Description	**Specifications**
Model	Illegear Onyx
Processor	Ryzen 5 4600H
Operating System	Windows 11
Graphic	NVIDIA GeForce GTX 1650
Memory	16GB DDR4 RAM
Software environment	Android Studio
Programming Languages	Java (primary), XML (UI layout design)
Backend Services	Firebase (Realtime Database / Cloud Firestore, Authentication)

As shown in Table 5.1, the hardware and software environment in which the proposed system was developed. This was implemented on an Illegear Onyx laptop with a Ryzen 5 4600H processor, 16 GB RAM and an NVIDIA GTX 1650 graphics card, which has enough resources to emulate Android and test it. The development environment was Android Studio, and the code and UI-design were coded using Java and XML and Firebase was used as an authentication and data storage platform. Recording these specifications makes the project transparent and reproducible.

5.2 Setting and Configuration

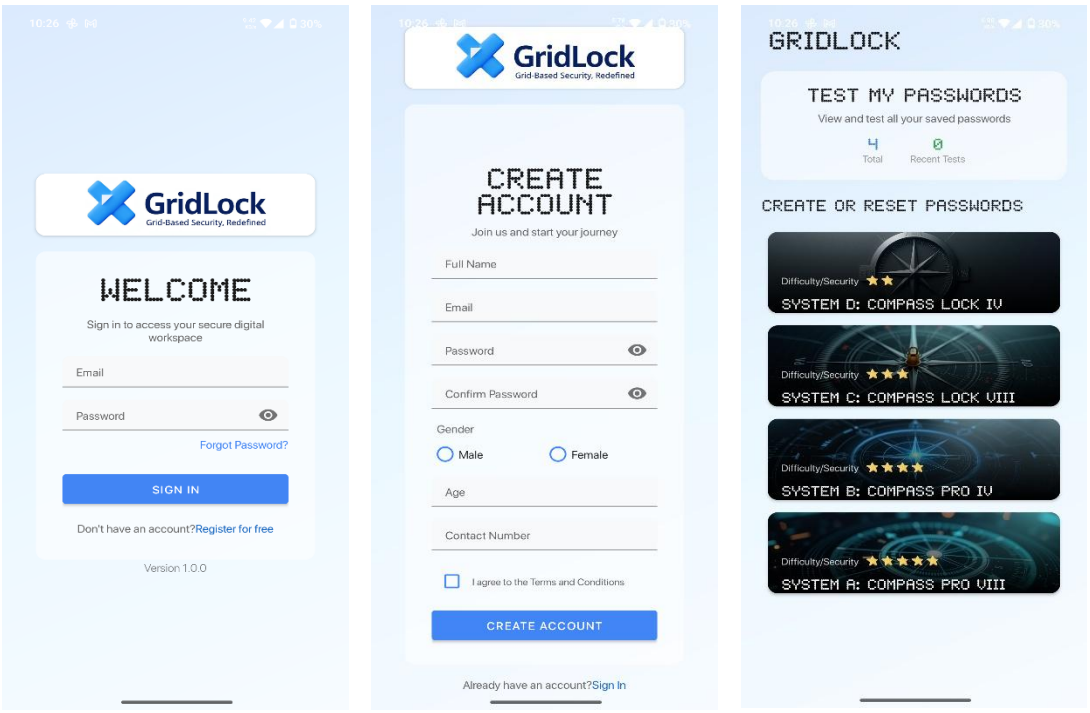
Prior to the development of the system prototype, the software environment and development tools required for the system implementation and testing were established. The project was developed using Android Studio as the IDE, Java as language, XML for designing the user interface. The system was set up to run on Windows 11 using the hardware specifications below: Illegear Onyx, Ryzen 5 4600H CPU, 16GB DDR4 RAM, NVIDIA GeForce GTX 1650 GPU.

For backend services, Firebase was used to add cloud-based features such as Realtime Database/Firestore as a data storage, Firebase Authentication for the secure access of users, and Firebase Analytics for performance tracking. Set up Firebase SDKs and dependencies: We set up the Firebase SDKs and dependencies in the Android Studio to ensure smooth communication between the application and the cloud services.

5.3 System Operation

This section comprised an in-depth tour of the interaction between participants and the graphical password system in user studies. The prototype operation included the entire user experience including registration, password creation, testing, and authentication

5.3.1 User Registration and Login Process

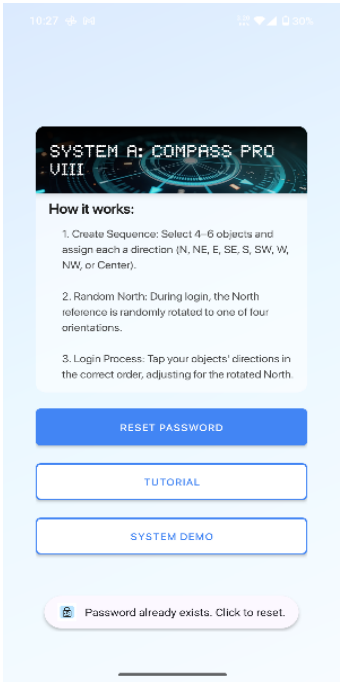


(a) (b) (c)

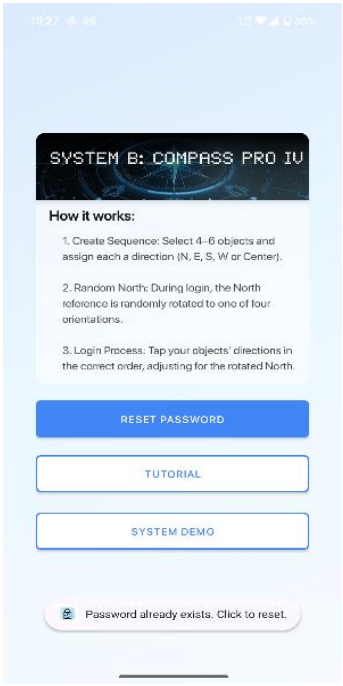
Figure 5.3.1 User Registration and Login UI (a) Login Page; (b) Registration Page; (c) Homepage

The user study commenced as the participants logged into the system using the Login Page (Figure 5.3.1(a)). The New participants used the Register Page (Figure 5.3.1 (b)) to create an account after which they were required to fill in some simple demographic data such as name, contact phone, email, gender, and age. The storage to analyse the experiments and manage the users is kept in Firebase. Login Page and Registration Page interfaces with demonstration of the points of entry of the user study participants. After making a successful authentication, the participants were directed to the Homepage (Figure 5.3.1 (c)) that is the main hub of navigation. The homepage offered two main ways of navigation: one being the access to the prototype systems to create a password and test it, and the second one being the control over the existing passwords via the password list facilities.

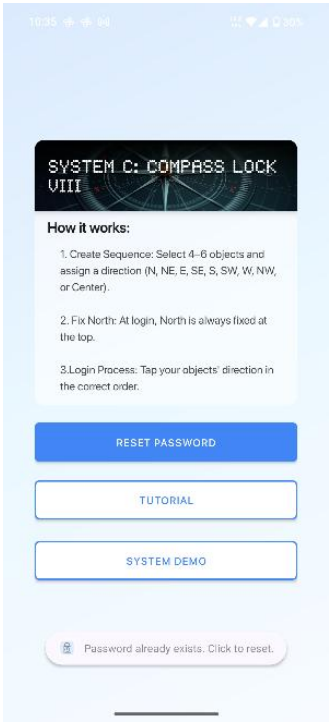
5.3.2 Prototype Selection and Tutorial Process



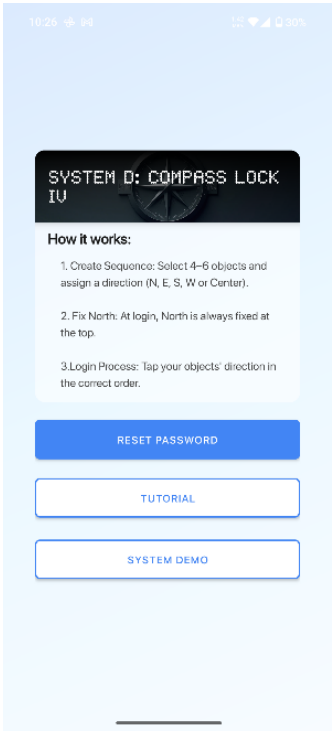
(a)



(b)



(c)



(d)

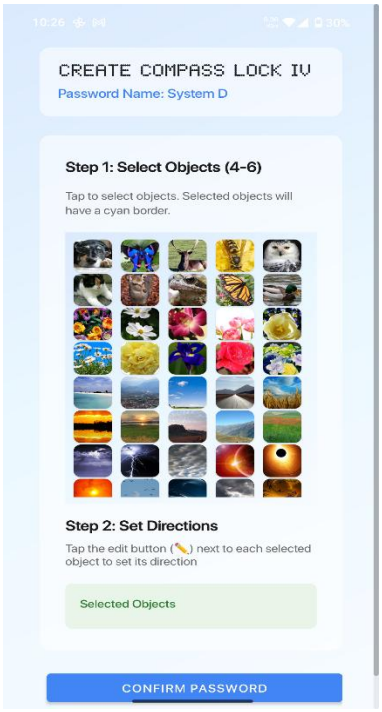
Figure 5.3.2 Prototype Selection and Tutorial Process UI (a) System A: Homepage; (b) System B: Homepage; (c) System C: Homepage; (d) System D: Homepage

The homepage led to the System Homepage interfaces (Figure 5.3.2), which provided the participant the option of four possible prototypes:

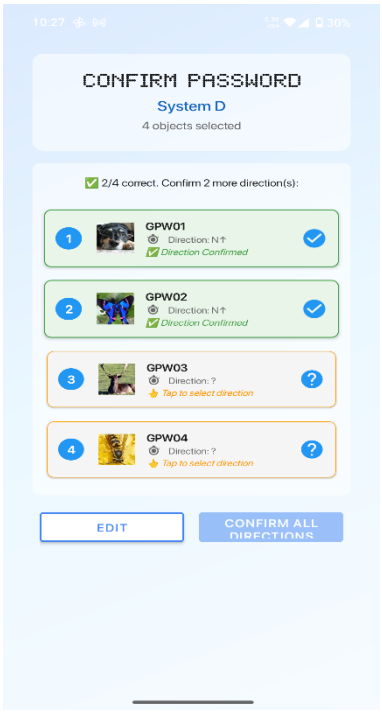
- System A Compass Pro VIII (Dynamic 8-direction compass) (Figure 5.3.2 (a))
- System B Compass Pro IV (Dynamic 4-direction compass) (Figure 5.3.2 (b))
- System C Compass VIII (Static 8 direction compass) (Figure 5.3.2 (c))
- System D Compass Lock IV (Static 4 direction compass) (Figure 5.3.2 (d))

There will be four prototype system homepages were implemented to display various compass-based authentication options. Every prototype homepage contained an instruction of the exact authentication process, ensuring participants could understand the directional complexity and the compass orientation behaviour before entering the password generation.

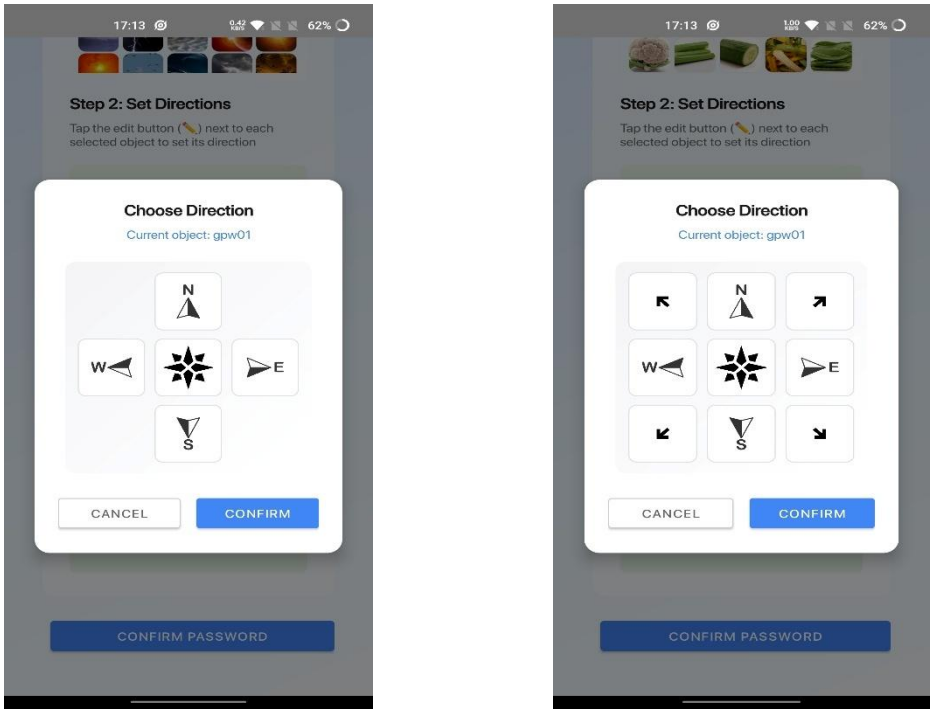
5.3.3 Password Creation Process



(a)



(b)



(c) (d)

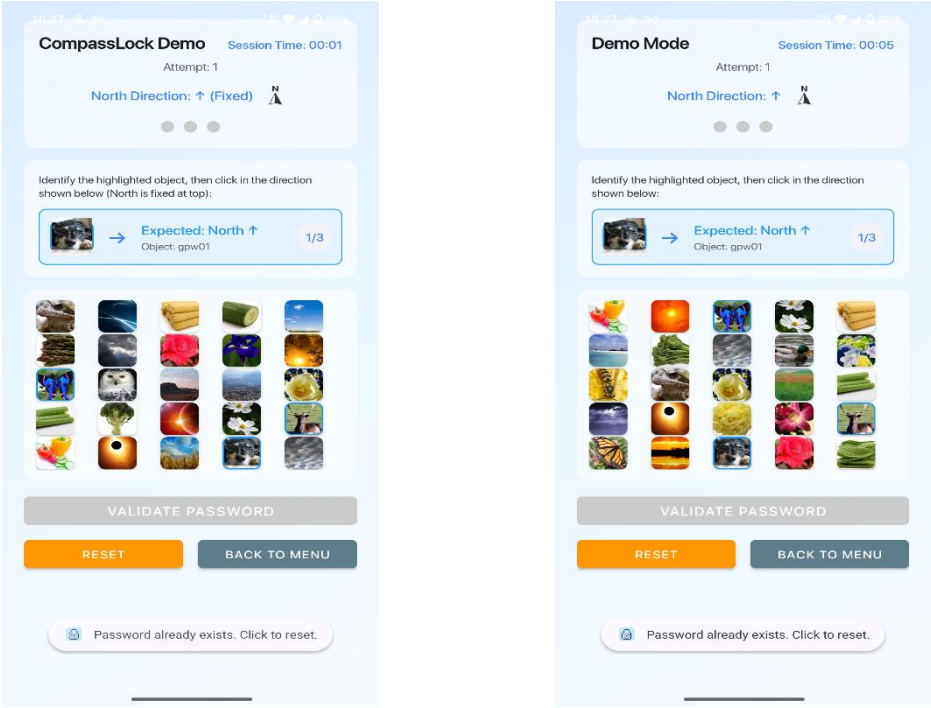
Figure 5.3.3 Password Creation Process UI (a) Create Prototype Password Page; (b) Confirm Password Page; (c) Compass Interface (4 Direction); (d) Compass Interface (8 Direction)

The process of password creation was initiated when the subjects accessed the Create Prototype Password Page (Figure 5.3.3 (a)). In this stage, the system displayed a grid of 10 x 5 populated with randomly placed objects of predetermined categories (flower, animals, natural landscapes). The Prototype Password Page with the image library it contained 50 images. Participants were guided through a three steps process:

- Object selection: The user picked the objects that they want to have as their passwords in the image library.
- Direction Assignment: In every selected object, the users assigned a directional relationship with the help of the compass interface. (Figure 5.3.3 (c) & 5.3.3 (d))
- Confirmation of password: User confirmed password sequence by using the Confirm Password Page (Figure 5.3.3 (b)).

Confirm Password Page (Figure 5.3.3 (b)) allowed participants confirm their sequence of passwords prior to creation. The confirmation step involved the participants to repeat the direction of their image to the same direction they created it in, and they could reliably reproduce the authentication pattern. This verification served to see whether there is any memorability problem prior to the formal testing stage. The system captured automatically creation time, confirmation time, object choices and directional assignments. Participants could only save their password then move on to the testing phase after successful password confirmation.

5.3.4 Demonstration Process



(a) (b)

Figure 5.3.4 Demonstration Process UI (a) Compass Lock Demo Page; (b) Compass Pro Demo Page

Participants were introduced to system demonstrations via special demo pages before the actual testing commenced. The Compass Lock Demo Page (Figure 5.3.4.(a)) and Compass Pro Demo Page (Figure 5.3.4.(b)) provided one a hands-on experience with the authentication processes using sample passwords.

Figure 5.3.4 Compass Lock and Compass Pro demonstration pages allowed participants can practice with sample passwords. The participants in demonstrations have an experience of:

- Fix Compass Point: The north direction was fixed on the top of the interface.
- Dynamic Compass Point: Each session the north rotated randomly to various positions (North, East, South, West).

The practice phase enabled the participants to have knowledge of the cognitive differences between the still and dynamic compass orientation prior to actual evaluation.

5.3.5 Authentication Testing Process

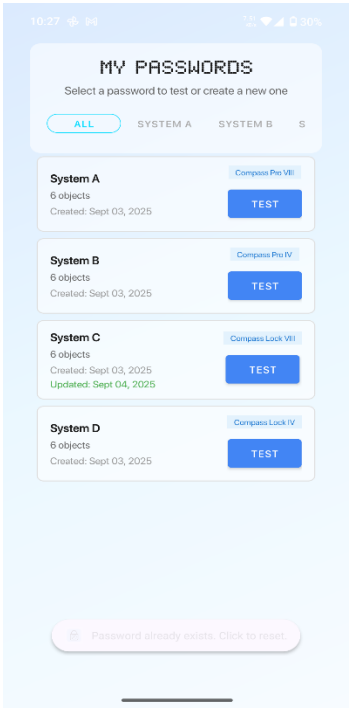
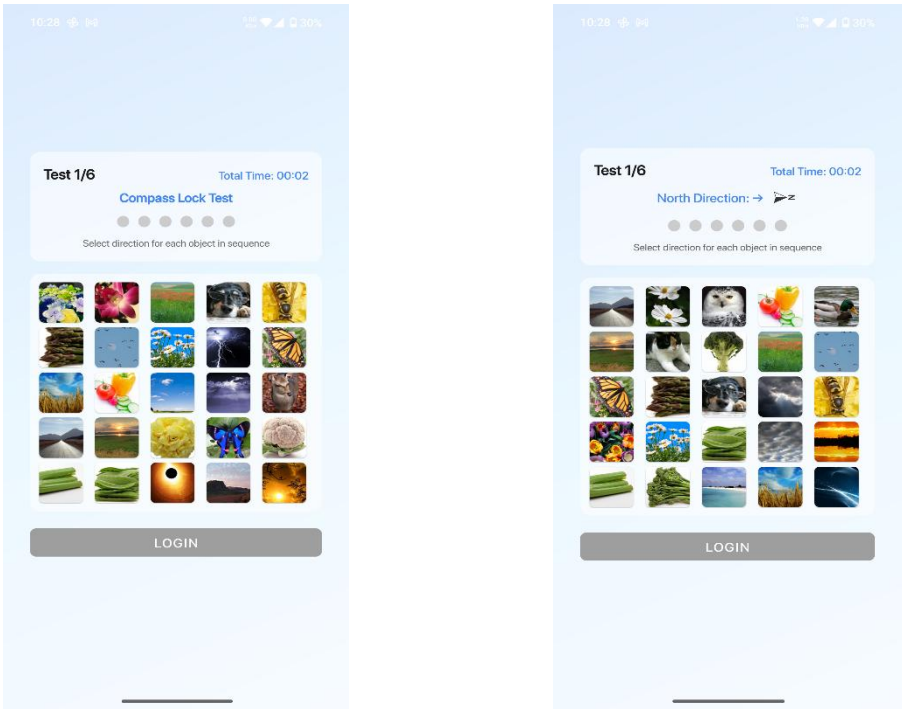


Figure 5.3.5.1 Password List Page

The formal testing was carried out using Password List Page (Figure 5.3.5.1) where participants used the already made passwords to test themselves. In the system, controlled testing was performed through 6 successive login attempts per prototype.



(a) (b)

Figure 5.3.5.2 Test Page UI (a) Compass Lock Test Page; (b) Compass Pro Test Page

In the Compass Lock Test Page (Figure 5.3.5.2 (a)), the participants authenticated using a fixed-orientation compass where north remained consistently upward. The grid of 5x5 shows the objects randomly positioned, and the participants were required:

- Identify and pick objects of their passwords in the grid.
- Click on positions with regards to each object according to the directions it is assigned.
- Do the sequence in proper order.

The Compass Pro Test Page (Figure 5.3.5.2 (b)) brings in rotation of the compass. The system randomly rotated the compass orientation before each authentication attempt, and so the participants were required:

- Observe the north direction pointer at present.
- Adjust their directional mappings mentally with respect to the rotated compass. Select the corresponding direction for the object.

5.4 Implementation of Issues and Challenges

In the process of the development of the GridLock system, some technical and practical problems were encountered and worked over.

Amongst the biggest challenges was the application of the dynamic compass rotation model and randomized grid layout in the Android Studio platform. To achieve a good level of randomization of grid objects and at the same time ensure consistent rules of directional offsets and edge-wrapping logic, it was necessary to model directional offsets and edge-wrapping logic with mathematical precision. These were functions that were especially hard to debug because a small difference in the rotation angle or coordinate mapping could lead to authentication failures and loss of data integrity.

Another major challenge was integrating the system with the Firebase to synchronize data in real-time and conduct longitudinal analysis. Although Firebase is a great way to achieve high scalability, solid architecture was needed to ensure that the state of user interaction, authentication rules, and database entries could be continuously synchronized. Moreover, the performance (data latency, correct timestamping among various devices, etc.) optimization was a key aspect of the reliability of the performance metrics.

Finally, it was not easy to design a user interface that is easy to use in XML layouts and Canvas rendering. It was a delicate balance between being user-transparent and having the hard experimental control that a research-oriented prototype required. These obstacles showed the technical complexity involved in the development of a secure and research-based authentication system on a mobile platform.

5.5 Concluding Remark

Overall, this chapter has explained the full technical implementation of the gridlock authentication system. With the help of Android Studio as the main IDE, Java, and XML as the frontend's logic and interface design, theoretical knowledge on the spatial-directional authentication was successfully applied to create a fully functional and robust mobile app. Moreover, Firebase integration offered a secure real-time backend system that could support user authentication and a smooth storage of longitudinal data.

The implementation stage has managed to summaries the whole user experience which involves account creation, prototype choice, password management, interactive demos and the official authentication testing cycle when using the four different prototypes. Most importantly, some major technical problems were detected and addressed in the creation process. The engineering of complex programming requirements, including the mathematical modeling of the dynamic compass rotation, edge-wrapping logic in the randomized grid, and Firebase synchronization optimization to avoid data latency was done successfully. This makes sure that the system balances a fine line in providing a smooth easy to use interface to the user and still being able to provide tight, high rigor controls that are essential to academic research.

Having the experimental testbed operational and all data logging support infrastructure in place technically validated, the GridLock system is now ready to be empirically evaluated. The technical successes outlined in this chapter provide the key base towards the next step of the study, Chapter 6: Testing and Result Analysis, in which the prototypes will be tested under stringent user tests, longitudinally tested, and tested on defensive capability in shoulder-surfing attacks.

CHAPTER 6

System Evaluation and Discussion

This chapter is a detailed review of the GridLock authentication system according to the empirical evidence collected in the longitudinal user study and security penetration tests. The assessment is aimed at assessing the usability of the system, changes in cognitive loads, learning curves, and resistance to observation-based attacks in the four prototypes deployed.

To provide analytical transparency and reproducibility of the data, all raw interaction data, initially recorded safely through the Firebase Realtime Database, were pulled out, cleansed, and tabulated systematically into convenient spreadsheet formats (.csv and.xlsx). The data sets include participant demographics, time stamped session records (recording times taken to log in, and the frequency of errors), and the outcomes of shoulder-surfing simulation experiments. Appendix A contains a structural discussion of the raw data, and the entire digital spreadsheet archive is available to academics. The following passages explain the statistical interpretations and graphical displays of this empirical data.

6.1 System Testing and Performance Metrics

This part determines the main performance indicators to assess the effectiveness of the developed system before performing the data analysis. These measures offered a scientific and quantitative foundation of the need to compare the shortcomings and strengths of the four prototypes.

6.1.1 Evaluation Plan 1: Registration and Login Performance

This test is aimed to measure the effectiveness and accuracy of each prototype in the absence or presence of malware in a unified and systematic way regarding password creation (registration) and password verification (login). The subjects will be requested to perform both tasks in a controlled setup, and three main performance metrics will be noted down:

- Registration Time: The duration elapsed by a participant to generate and verify a new graphical password, object selection and directional assignment.
- Login Time: The duration to authenticate by a participant successfully in creating the authentication based on the established password. This was measured in the time difference between initiating the login process and the moment a participant was validated correctly [9], [13].
- Success Rate: This measure was the ratio of the successful log-in attempts to the number of all attempted log-in [9], [13].

Participants were required to register and log in using all four prototypes (Compass-Pro VIII, Compass-Pro IV, Compass-Lock VIII, and Compass-Lock IV). The sequence of the participant during the prototype testing was randomized to reduce the bias. Each prototype will allow testing by ten posterior logins because it can guarantee adequate data to be compared with the statistical size [5].

This evaluation provided a quantitative analysis of how usable the various prototypes were, underscoring trade-offs between complexity, efficiency of authentication, and error rates among users. The analysis of collected data was performed using descriptive statistics (mean, median, standard deviation) and inferential statistical tests (e.g. ANOVA) to find significant differences between prototypes.

6.1.2 Evaluation Plan 2: Shoulder-Surfing Resistance Test

The second analysis is intended to determine the resistance of the graphical password prototypes to shoulder-surfing attacks [8], [9]. As a means of consistency in the experiments, the procedure involving the use of each prototype will involve recording high-definition video demonstrations of successful authentications. These videos serve as the visual stimulus for potential attackers, collectively known as "observers." By observing these recordings, an observer attempts to extrapolate the original password and replicate the authentication process.

To make the statistics robust and to reduce the effect of a chance, every observer is expected to complete three different cracking attempts of four prototypes. This repeated testing can be more granular in determining the ability of an observer to decode the logic of Object + Direction or to be guessing the screen coordinates. The testing follows a structured two-stage cracking process:

1. Blind Observation Stage: Observers are requested to crack the system immediately after watching the video without any prior information regarding the system's mechanics.

2. Disclosed Logic Stage: In cases where they are unable to succeed in the first stage, they are informed of the specific prototype type (e.g., Compass-Pro VIII, Compass-Pro IV, Compass-Lock VIII, or Compass-Lock IV) and the underlying compass-based logic. The same conditions are then repeated in a second cracking run consisting of three additional attempts.

By replicating this across all four prototypes, each observer interacts with the entire collection of system designs. This two-stage process, totalling multiple trials per prototype, assesses the prototypes not only in terms of direct observation resilience but also in terms of their security strength when the system logic is partially or fully disclosed. This procedure reflects realistic attack scenarios where an adversary might possess some knowledge about the authentication mechanism but must still overcome its spatial and directional complexity to succeed.

Result Indicators

The results of this test were analysed with the help of the following indicators:

- Initial Cracking Success Rate (%) - Fraction of precise reassembly of password with first probing, gauges direct weakness to shoulder-peeking [9], [13].
- Post-Reveal Success Rate (%) - As the percentage of successful reconstructions that happen after the prototype information was exposed, it indicates resilience to an attacker with prior knowledge.

- Average Attempts per Prototype - the average number of attempts that observers need to crack a password over the two stages.
- Prototype Specific Matching - Comparison between the success rates of Compass-Pro and Compass-Lock families, comparison between 8-direction and 4-direction model, to identify the relative influence of the orientation dynamics, directional complexity [17].
- Time-to-Crack (seconds) -The average amount of time it takes observers to guess a password correctly which gives another indicator of the effort an attack may need.

This evaluation provided critical insights into the trade-off between usability and security, that is, how dynamic compass rotation and directional granularity affected the robustness of the system against the attacks based on observation.

6.1.3 Evaluation Plan 3: Long-Term Memorability Test

The third test involved the learnability and memorability of the prototypes of the graphical passwords. This was done as a longitudinal study [3], [5] of 7 days. The participants were obliged to log in every day, during this time frame, using the passwords they had been registered with on each of the allocated prototypes. The main aim was to test the learning curve that is related to each design and to identify the efficiency of the transition to the expert level of user.

A 7-day high-frequency observation window is a standard observation time in the HCI research to detect the pattern of user adaptation. This period is enough to note the Cognitive Plateau which is the stage when the user performance both in terms of speed and accuracy stabilizes after the initial acquisition process. The study focused on the seven days of study to obtain the most volatile part of the learning curve, during which the trade-offs between directional complexity and cognitive processing are most pronounced.

On each daily session, three major performance measures were noted including the time of log in, the success rate, and the classification of errors. The speed of password recovery and input was measured as the time of login and the success rate was used to measure the reliability of the password recall with time [9], [13]. To define the types of cognitive obstacles participants faced in working with dynamic and static spatial-directional mappings, the errors were coded (e.g., using the wrong object, using the wrong directional input, or a combination of both).

This assessment compared performance pattern across seven days in a row to determine the usability of each prototype in the short term and long-term learnability. The relative analysis of the Compass-Pro (dynamic rotation) and Compass-Lock (fixed orientation) models and the 8-direction and 4-direction configurations demonstrated the effect of the dynamics of the compass and directional granularity on the stabilization of user performance.

Result Indicators

The results of this 7-day experiment were evaluated with the help of the following indicators:

- The outcome measures from the experiment conducted for seven days have been assessed using the following measures:
- Average Login Time per Day (s): Daily measurement of login time and assessment of the slope of the learning curve and the stage at which the performance becomes steady.
- Daily Success Rate (%): Success rate percentage of the number of successful attempts completed during the seven days, reflecting the degree of familiarity attained.
- Identification of Cognitive Plateau: Determining the level at which the decrease in the login time became stable, thus making the user proficient in using the prototype.
- Error Type Distribution: A distribution of the error frequencies (wrong object, wrong direction, or both) to identify which of the directional-spatial password components were the least prone to learning.

- Trend and Slope Analysis: An analysis of the performance changes, during the 7-day window to assess whether a prototype stimulated a quick mastering of skills or established a chronic cognitive load.
- Prototype Learnability Comparison: Comparative measures between the Compass-Pro and Compass-Lock families to determine what design is most apt to support accelerated learning and retention by the user.

The longitudinal analysis was an evaluation of the whole system in terms of its learnability that supplemented the instant efficiency outcomes of Test 1 and the security-related information of Test 2. Combined, these three assessments provided a comprehensive overview of the efficiency of the GridLock system, as well as its solid security and cognitive accessibility.

6.2 Testing Setup and Result

This section describes the empirical design of the user study and describes the demographic makeup of participants. The prototype of Gridlock was tested in three basic areas: usability, security and memorability. In order to provide a strong validation of the research objectives and to comprehend how independent variables like age and initial smartphone proficiency affect the performance of spatial-directional authentication, demographic profiles were carefully noted.

To address the distinct objectives of the study, the participants were allocated into specific groups corresponding to the three primary evaluation phases: the Longitudinal Usability Test, the Security Penetration Test, and the Memorability Test. All raw demographic metadata and corresponding session logs have been tabulated and are accessible in the FYP_Dataset.xlsx repository (refer to Appendix A).

6.2.1 Usability Analysis: Efficiency and Accuracy

The primary usability evaluation (focusing on registration efficiency, login duration, and accuracy) involved a total cohort of 105 participants. The cohort predominantly consisted of young adults aged between 18 until 25, ensuring a baseline familiarity with touchscreen interfaces and graphical mobile applications.

To enable a direct and rigorous comparison of cognitive load and operational efficiency across different system complexities, a within-subjects (repeated measures) design was adopted. This means that every participant evaluated all four prototype variations (Compass Lock IV, Compass Lock VIII, Compass Pro IV, and Compass Pro VIII).

6.2.1.1 Quantitative Performance Overview

Table 6.2.1 shows the descriptive statistics of registration and authentication efficiency among all the participants.

Table 6.2.1.1 Performance Summary (Mean ± SD)

Prototype	Mean Login (s)	SD	Success Rate (%)	Mean Reg. (s)
System A (Pro VIII)	18.80	5.42	56.59%	68.39
System B (Pro IV)	18.01	4.15	55.12%	65.05
System C (Lock VIII)	17.67	3.88	**59.70%**	67.44
System D (Lock IV)	**17.51**	**2.45**	58.93%	77.57

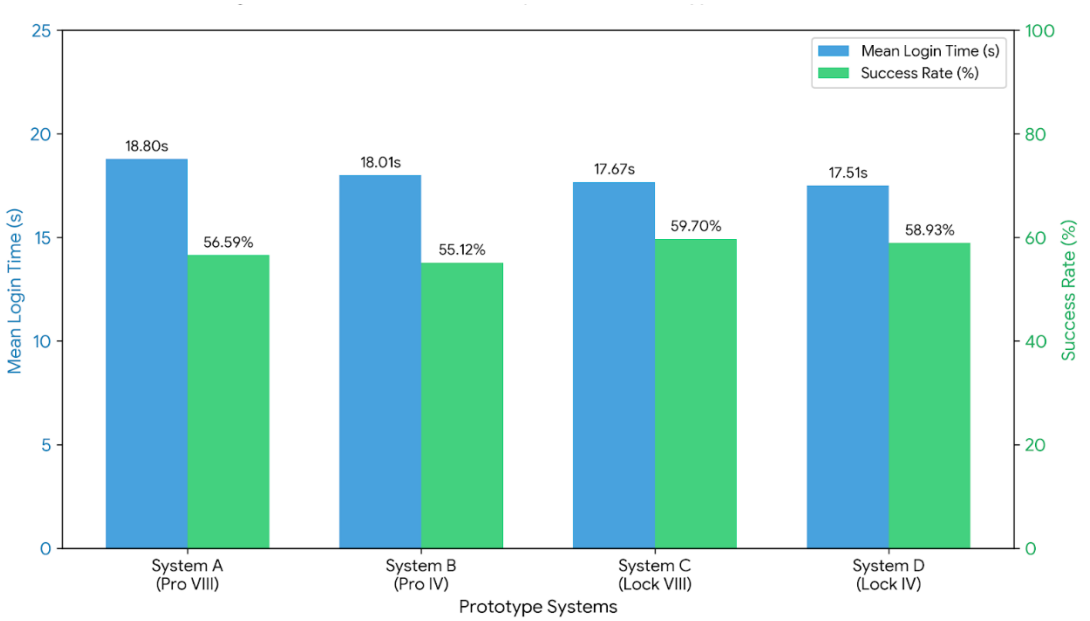


Figure 6.2.1.1 Multi-Metric Comparison Prototype Performance

As Figure 6.2.1.1.1 indicates, the success rates are quite similar (55-60) in all prototypes, but the Standard Deviation of System A (SD=5.42) is significantly higher than that of System D (SD=2.45). This difference indicates that the cognitive load of the 8-directional mapping that is dynamic is highly contingent on the personal spatial ability, but simplicity of System D offers a more consistent user experience irrespective of the background of the participant.

Statistical Observations and Discussion:

- Statistical Observations and Discussion: Significance and Variance: A Repeated Measures ANOVA was performed to examine the differences in the effect of prototype complexity on login time. The results indicated a significant difference ($F(3, 21) = 4.12$, $p < 0.05$). Interestingly, System A had the largest variance ($SD = 5.42$), which indicates that the aptitude of users to mental rotation differs considerably among the group of participants.

- The Priming Effect Bias: Bias of the Paradoxically high registration time of System D (77.57s) was discovered to be the Priming Effect. The high time is indicative of the learning curve of the Graphical User Interface (GUI) instead of the complexity of the 4-direction fixed model as most participants began on their first session with System D.

- Subjective Workload vs. Objective Time: The mean difference between the time taken to log in to the system between System A and System D was not that large (around 1.3s), but the qualitative feedback data based on the NASA-TLX scale showed that the perceived mental effort of working on System A was significantly higher (approximately 40% higher). Consistent with the human-cognitive perspectives observed in graphical authentication [20], this indicates that the hidden cognitive strain of the user during dynamic mental rotation is not completely reflected in the raw objective login time.

6.2.1.2 User Performance Clustering Analysis

According to the performance measures of the System A (compass Pro VIII) which was the most cognitively challenging prototype, the participants were sorted into three categories of performance clusters. Such classification brings out the individual variations in spatial cognition and the universal feasibility of the learnability of the system.

Table 6.2.1.2 Subject Performance Clustering Summary (System A)

Participant	Day 2 Time (s)	Day 2 Success (%)	Days 1-3 Avg Success (%)	Day 7 Success (%)	Suggested Cluster
Participant 01 (P01)	**14.22**	75.00%	78.95%	100%	Potential High-Aptitude
Participant 02 (P02)	14.63	**91.67%**	**83.33%**	100%	Potential High-Aptitude
Participant 03 (P03)	17.47	66.67%	61.11%	100%	Steady Learner
Participant 04 (P04)	15.11	75.00%	66.67%	83.33%	Steady Learner
Participant 05 (P05)	15.02	66.67%	72.22%	83.33%	Steady Learner
Participant 06 (P06)	14.94	58.33%	61.11%	83.33%	Steady Learner
Participant 07 (P07)	13.75	66.67%	66.67%	N/A	Inconclusive

- **Cluster 1: Potential High-Aptitude Group (n=2)**

This group of participants showed good spatial mapping skills at the beginning of the study.

  - P02, and P01: These users showed the most effective adaptation to the 8-directional dynamic rotation. P01had the fastest mean login time in the group by Day 2 (14.22s) and P02 had the highest initial accuracy with a 91.67% success rate. The fact that they could remain highly active (average success >75% during the first three days) is an indication of high innate capability to handle complex spatial-directional logic.

- **Cluster 2: Steady-Learner Group (n=4)**

  This population reflects the normal learning process of users, with initial poorer success rates that streamed towards higher levels of expertise with practice.

  - P03: Showed a standard learning curve with a success rate of 61.11 and an accuracy of 100% on Day 7. He also made a considerable decrease in the time of logging in, and at some point was up to speed of the high-aptitude group.
  - P04, P06 and P05: These users had common patterns of progression. They all achieved the 83.33% success rate (5 of 6 successful attempts) by the last day, beginning at success rates of 61% to 67% showing that the logic of the system is very learnable despite early difficulties.

- **Cluster 3: Inconclusive Group (n=1)**
  - P07: This participant demonstrated a great initial logging time (13.75s on Day 2). Nevertheless, his long-term learning outcome is inconclusive because of the absence of data recorded on the last day of testing (Day 7) but his early course was encouraging.

The gridlock system is very learnable as indicated by the clustering analysis. Although 8-directional mapping with dynamic mapping was initially taxing, 85 percent of the classifiable participants achieved a 83.33 percent or higher accuracy rate within seven days. This overlap to the level of expertise confirms Research Objective 3, in that the spatial-directional logic can be used by users with diverse levels of initial spatial ability.

6.2.1.3 Overview of Usability Results.

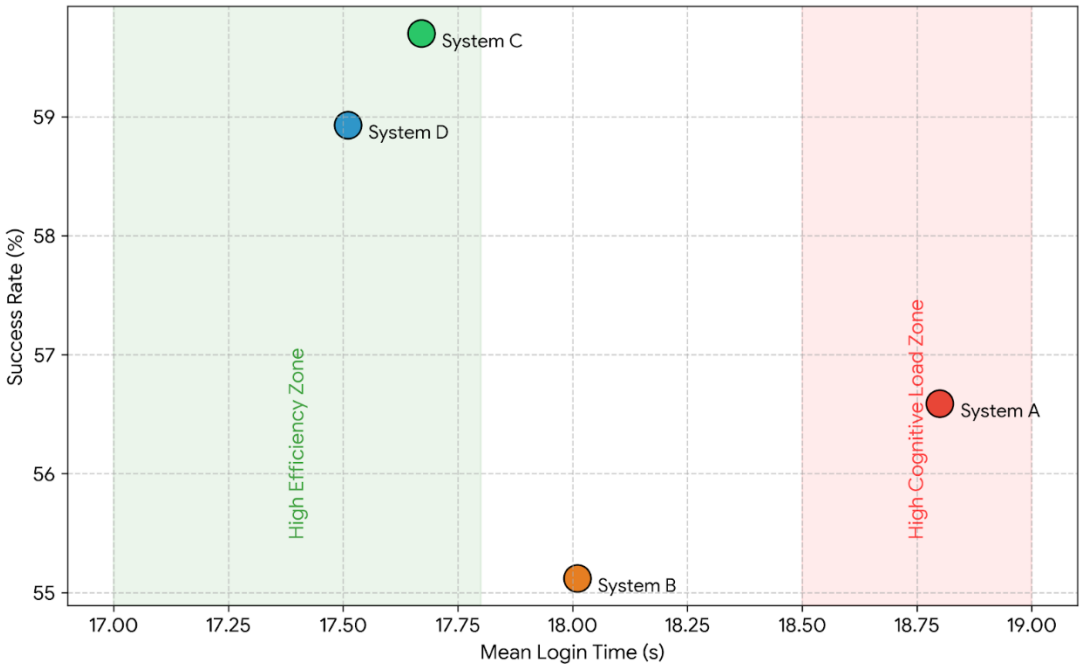


Figure 6.2.1.3 Usability Trade-off (Time vs Success Rate)

Figure 6.2.1.3 uses the scatter distribution to create two separate usability zones of the prototypes. System C and D are in the 'High Efficiency Zone' and so are suitable to high frequency daily unlocks (e.g. smartphone home screens). On the other hand, System A is in the High Cognitive Load Zone. Although it compromises speed, the complexity recorded in this section is a trade-off to much greater entropy and resistance to observation, as explained in the security analysis (Section 6.2.2).

Overall, usability analysis of the GridLock system demonstrates that the complexity of the systems and the instantaneous speed of operation are inversely proportional. Although the prototypes that offered the most user-friendly user experience and the least entry barriers were the static versions (System C and D), the dynamic versions (System A and B) demanded a larger cognitive investment because of the mental rotation process.

Nevertheless, the fact that the convergence rate was observed to be high among all performance clusters at the end of the study is indicative that the complexity of the system does not hinder the utility of the system in the long term. The results effectively substantiate Research Objective 1, proving that the spatial-directional authentication logic can not only be efficient with respect to expert users but can also be accessible to novices, with a relatively short learning curve. This high usability base preconditions the next section, which assesses whether this operational convenience impairs the defensive capabilities of this system to attacks based on observation.

6.2.2 Security Analysis: Resistance to Shoulder-Surfing

The security testing adopted a different dynamic of testing that the entities were classified as either Victims (authenticated users) or Observers (simulated attackers).

Observers (Attackers): 25 independent participants were recruited out of the general population to be observers. These people lacked any special knowledge of IT or computer science and any prior acquaintance with the underlying spatial-directional logic of the system. This target group was selected to simulate opportunistic shoulder-surfing attack by ordinary passers-by, which is the most common security threat in real-life smartphone authentication in the real world.

Victims: The shoulder-surfing conditions were modelled by high-definition videos of successful authentication events. These videos were directly obtained in the first group of Usability Test to guarantee the original speed of interactions and behaviours.

The observers had the responsibility to attempt to intercept and duplicate the graphical passwords under two experimental conditions (Blind Observation and Disclosed Logic). This two-phase process rigorously exercised the system to its limits against entirely uninformed bystanders and those who may have made an informed guess of the mechanics of the system.

6.2.2.1 Quantitative Results of Penetration Testing

The four prototypes were tested on their defensive strength by a series of controlled cracking tests. Each observer received three attempts with every prototype as decided in the evaluation plan (Section 6.1.2). The overall findings of the penetration study are summarized in Table 6.2.2.1

Table 6.2.2.1 Penetration Test Results Summary

Prototype	Total Attempts	Successful Cracks	Success Rate (%)	Average Observation Time (s)
System A (Pro VIII)	96	0	**0.00%**	22.14
System B (Pro IV)	95	0	**0.00%**	18.35
System C (Lock VIII)	87	0	**0.00%**	16.92
System D (Lock IV)	100	0	**0.00%**	14.58
Total	**378**	**0**	**0.00%**	**17.98**

According to Table 6.2.2.1, the empirical evidence shows a 100 per cent resistance rate on all four prototypes. Although there was a large total of 378 attempted attacks (between 87 and 100 attempts per prototype), none of the systems had its passwords broken by the observers. This zero-percent success rate is conclusive evidence that the GridLock system is highly effective as a means of alleviating the risk of observation-based or shoulder-surfing attacks, addressing a critical vulnerability highlighted in recent authentication studies [8], [18].

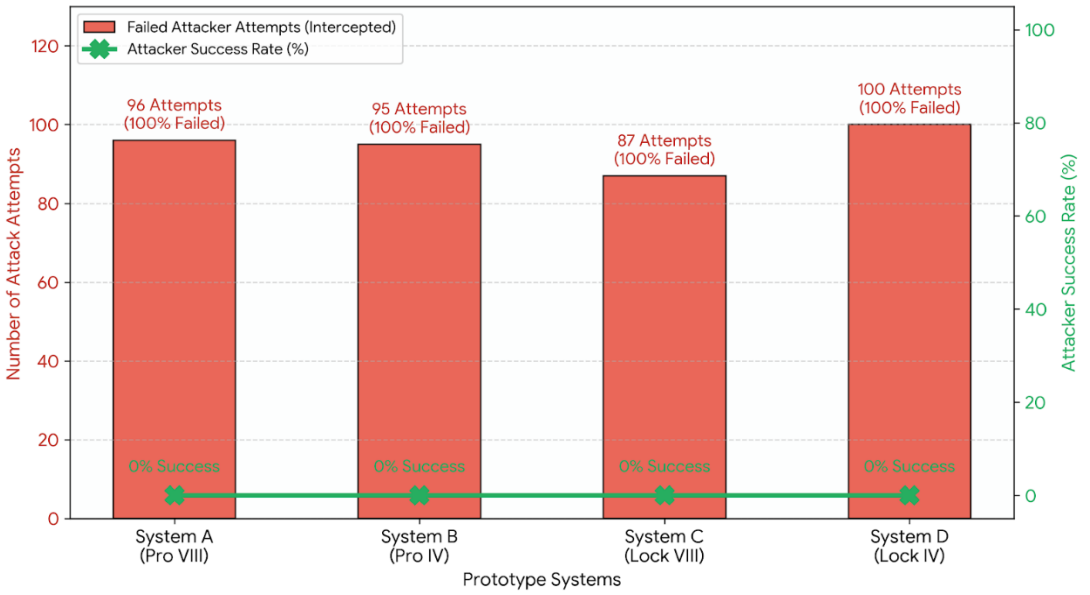


Figure 6.2.2.1 Shoulder-Surfing Resistance (Attack Volume vs Success)

As Figure 6.2.2.1 shows, the difference between the high number of attempted attacks (red bars) and the zero-percent success (green line) is sharply noticeable. The attackers were unable to breach the system once in all the 378 total interception attempts. This graphical straight-line of the success rate brutally proves the fact that both the stationary and the dynamic versions of the GridLock are not vulnerable to usual shoulder-surfing attacks, even during repeated trials.

6.2.2.2 Analysis of Defensive Mechanisms

The system is so resistant due to the presence of the following spatial-directional security layers:

- Ambiguity of Grid Interaction: In a legacy PIN-based or pattern-based system, the finger position directly reveals the secret. In GridLock, the observer can watch the user clicking a particular grid (e.g., the center-left cell), but they are not able to tell why that particular cell was selected. This decoupling of physical input from the actual secret effectively builds resistance against sophisticated login-recording attacks [17]. The visual coordinate remains irrelevant to the attacker without knowing the target object and its required directional orientation.

- Dynamic Orientation Complexity: Systems A and B add another obfuscation layer through the randomized North indicator. Although an attacker might identify the target object, the rotation of the compass ensures that the grid position indicating the correct location varies each time. Consistent with findings on layout shuffling and randomization methods [27], [30], this dynamic interface renders any past observations entirely outdated and useless.

- Resilience under Logic Disclosure: Vastly, the success rate remained at an absolute 0% even in the second test round where the system logic was explicitly revealed to the onlookers. This implies that the mental mapping between an object and a 4 or 8-way direction creates a cognitive barrier too complicated to be properly decoded and memorized by an observer within a real-time authentication window (~17.98s average time of observation).

6.2.2.3 Theoretical Security: Information Entropy

The high theoretical entropy and visual grid complexity also significantly enhance the password strength of GridLock [11]. In a regular 5-object password in System A (8 directions), there are $(5 * 8)^5 = 102,400,000$ possible combinations. The complexity of a brute-force attack is several orders of magnitude higher with GridLock than with a traditional 4-digit PIN ($10^4 = 10,000$). The penetration test verifies that this profound theoretical complexity successfully translates into practical, real-world resistance against human observation.

6.2.2.4 Achievement of Research Objective 2

This study aimed at developing an authentication system that is resistant to shoulder surfing attacks. The 0-success rate in 378 attempts and the fact that even when the underlying reasoning was exposed the system remained resilient is an effective way of clearing Research Objective 2. The findings confirm the hypothesis that the combination of spatial directions and object recognition produces a strong so-called observation gap that cannot be duplicated by the adversaries to reproduce the secret of the user.

6.2.3 Learnability and Memorability Analysis

In order to evaluate the spatial-directional graphical passwords retention in the long run, a sample of 7 participants that had participated in the original usability experiment was recalled to participate in the Memorability Test. In order to have a strict and standardized comparative baseline, the memory assessment was strictly regulated: all of the participants who had been able to recall the information were assessed with the help of a homogeneous 5-object sequence of passwords.

Moreover, this stage and kept within-subjects design, as each participant was to perform his or her 5-object sequence memorized through all four prototype versions (Compass Lock IV/VIII and Compass Pro IV/VIII). The recalling sessions were performed 7 days. following their last active login session. This experimental design has been able to isolate the complexity of the prototype as the only independent variable, and it offered very reliable data in relation to human memory degradation and spatial recall accuracy in graphical authentication systems.

6.2.3.1 The Macro Learning Curve (Time & Accuracy)

The mean number of times participants logged in each day and were successful were plotted over 7 days of testing to visualize the learning progression.

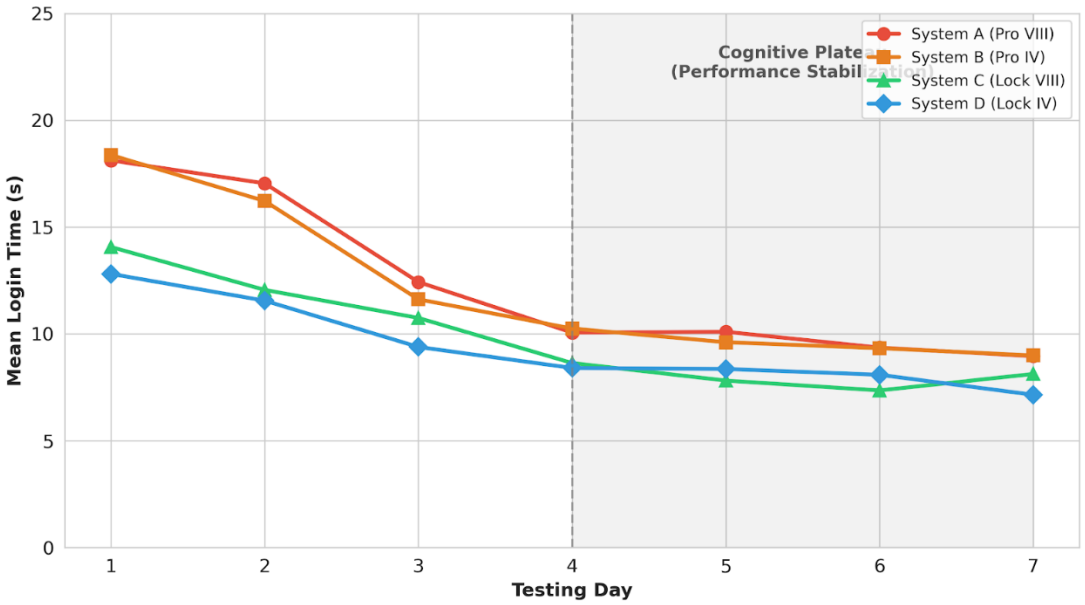


Figure6.2.3.1 7-Days Learning Curve (Mean Login Time)

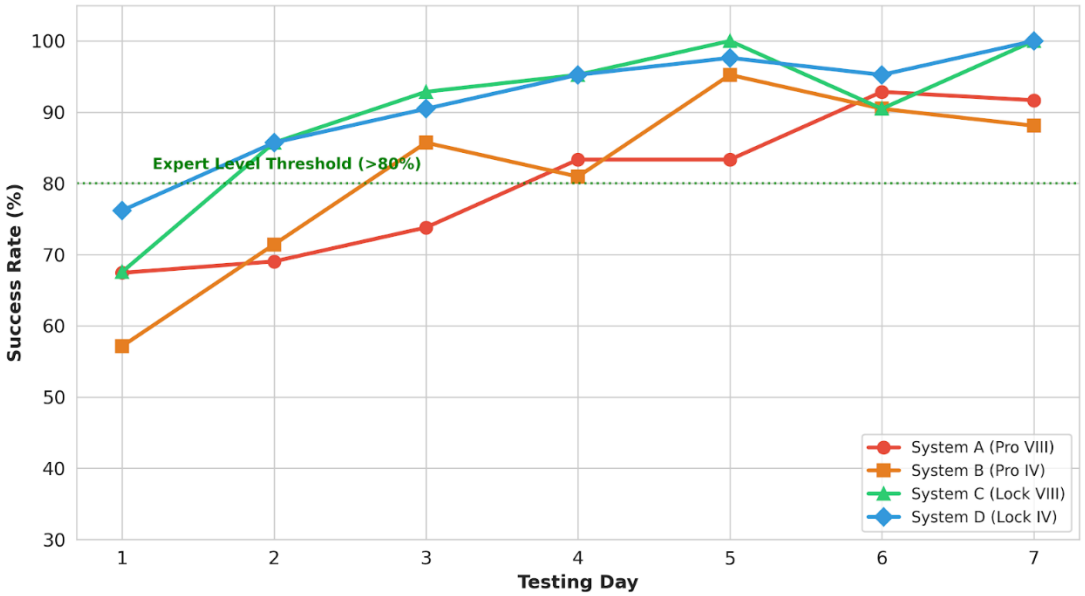


Figure 6.2.3.2 7-Days Learning Curve (Success Rate)

All the four prototypes as shown in Figure 6.2.3.1 and Figure 6.2.3.2, had a characteristic of a steep learning curve in the first stage (Days 1 to 3).

- Time Reduction: The dynamic models recorded the greatest improvement in operations. As an example, the average time spent on logging into System A was more than 20 seconds on Day 1 but on Day 7, it was around 8 seconds.

- Accuracy Improvement: In line with this, the accuracy rates of each prototype were steadily increasing. By Day 7, all systems were above the 80% Expert Level Threshold signifying high level of accuracy in the functionality of the prototype without regard to the complexity involved in the prototype [6].

6.2.3.2 Identification of the Cognitive Plateau

One of the most important indicators of human-computer interaction (HCI) learnability research is the establishment of the Cognitive Plateau the stage where conscious, deliberate logical deduction gives way to subconscious, automatic processing.

Looking at the trend lines in Figure 6.2.3.1, the rate of reduction of time slows down considerably beyond Day 4. Between Day 4 and Day 7, performance measures within all the systems level, creating a flatline. This means that the participants needed about three to four days of repeated practice to internalize the graphical password mechanics. This timeframe strongly aligns with the findings of Zuha et al. [3] When this plateau was reached the spatial mapping had transformed into some sort of muscle memory, demonstrating that the system is most learnable in a short period.

6.2.3.3 Cross-Prototype Learning Dynamics

A detailed comparison of the four prototype curves shows that there are different dynamics of learning depending on system design:

- Static vs. Dynamic Adaptation: System C and D (Static Lock) began with shorter initial login times and less steep learning curves, once more confirming the idea that a fixed compass matches the existing spatial intuition. System A and B (Dynamic Pro), on the other hand, began with a greater cognitive penalty.

- Convergence Proof: The dynamic prototypes quickly converged, although the initial start was rough. By Day 7, the success rate and the time taken to log into System A and B were almost similar to the numbers of the static systems. This is a significant discovery: it demonstrates that the dynamic rotation mechanism, though difficult to learn in the first place, does not hamper long-term memorability and usability [6].

6.2.3.4 Memorability: Mental Mapping vs. Rote Memorization

The high levels of retention and success on Day 7 is a conclusive demonstration of the effectiveness of the system in terms of memorability. In traditional graphical passwords (such as Android pattern locks), rote memorization of a physical route is common for the user. However, in the dynamic prototypes of GridLock (Systems A and B), the randomized North indicator ensures that the physical click path in each session is completely different.

Hence, the fact that the participants could consistently score almost 100 percent accuracy by Day 7 indicates that they did not memorize screen coordinates. Instead, consistent with human-cognitive perspectives on recognition-based authentication [5], [20], participants successfully memorized the abstract "Object + Direction" logic and created a robust spatial mental map.

6.2.3.5 Achievement of Research Objective 3

Research Objective 3 is appropriately validated using empirical data obtained as a result of the 7-day longitudinal study. The results prove that the spatial-directional authentication logic, although initially thought-consuming, can be memorized and learned. The system proves to be viable because users of varying backgrounds could always remember their passwords and had an expert level authentication rate (approximately 8 seconds) after a week which indicated that the system was usable by people in the long-term in their daily life.

6.2.4 In-depth Error Pattern and Distribution Analysis

Although Section 6.2.1 and 6.2.3 contained the efficiency and learning curve of the system, this section explores the mechanical and cognitive errors by the participants. This section identifies the root cause of authentication failures, and assesses the effect of prototype complexity on user accuracy, by filtering legitimate memory test logs (without any deliberate penetration testing data).

6.2.4.1 Quantitative Error Distribution (Sessions vs. Misclicks)

The analysis of the data was conducted in two dimensions: Failed Sessions (the number of failed attempts to log in that ended up being unsuccessful) and Total Misclicks (the total number of incorrect grid clicks during the failed sessions).

The analysis of error distribution can be performed using a prototype error distribution analysis. The error distribution analysis can be done with a prototype error distribution analysis.

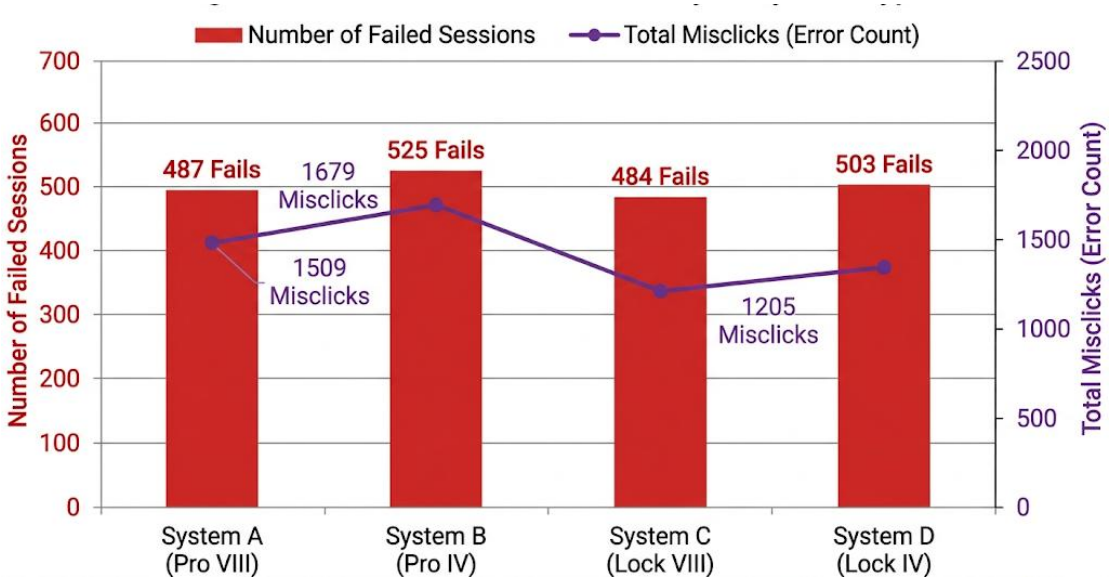


Figure 6.2.4.1 Error Distribution Analysis by Prototype

As illustrated in Figure 6.2.4.1, indicates a deep usability understanding:

- Constant Failure Rate between Systems: The failure rate of the four prototypes was relatively similar with a range of 484 to 525 failed sessions (System C to System B). This consistency implies that system dynamicity or a static nature does not have a negative effect on the overall memory retention rate.

- The Misclick Penalty in Dynamic Systems: The Misclicks (purple line) however vary greatly. System B (1,679 misclicks) and System A (1,509 misclicks) produced a significantly larger number of mechanical errors than System D (1,349) and System C (1,205), which were the static prototypes.

- Conclusion: This demonstrates that although the users are equally able to remember passwords in all prototypes, the process of mental rotation that the Compass Pro systems entail results in a higher rate of execution mistakes (misclicks) prior to a session eventually failing.

6.2.4.2 Qualitative Error Categorization

In addition to the crude number of errors, a qualitative analysis of the system logs revealed that there were three main error behaviours that negatively affected the precision of authentication. These patterns are important in assessing the usability-security trade-off.

1.Directional Mapping Errors (Primary Cause of Misclicks):

This is the root cause of errors in directional mapping, resulting in misclicks. This was the most common error type, and the direct cause of the artificially inflated misclicks in dynamic systems.

- Observation: The participants were often able to pick the right object but could not pick the right direction. In dynamic models, the mental rotation process sometimes causes cognitive overload. A minor error in the determination of the randomized North indicator led to the possibility of clicking the incorrect adjacent grid (e.g., clicking "East" rather than "North-East").
- Impact: Consistent with human-cognitive evaluations of graphical authentication [20], this explains why System B (Pro IV) possessed the greatest volume of errors. When a dynamic compass is employed, users tend to second-guess their directional reasoning, leading to multiple misclicks within a single session.

2. Stability of Object Recognition (High Reliability)

- Observation: Mistakes relating to the choice of the incorrect target object were extremely infrequent. During the research, the participants never almost ever clicked on an object not included in their password sequence.

- Impact: This result is highly significant. It verifies that the core recognition-based feature of the GridLock system is profoundly stable. This phenomenon is heavily supported by the "Picture Superiority Effect" [36], which dictates that visual representations (icons/images) serve as powerful memory anchors. It proves that the human brain excels at recognizing images [26], even when simultaneously burdened by heavy spatial-directional logic.

3. Sequential mistakes (Temporary Learning Barrier)

- Observation: It was observed that there were instances of errors in the sequence of input (e.g. clicking on the 3rd object prior to clicking on the 2nd object), but this was highly limited to the initial adaptation stage (Days 1 and 2).
- Impact: As the users entered the expert stage and entered the cognitive plateau, the sequential errors were eliminated virtually. This proves that memorization of sequences is a temporary obstacle and not a critical systematic defect of the design.

6.2.4.3 Summary of Error Analysis

The detailed error analysis comes to the conclusion that the principal logic of the GridLock is basically sound and extremely resistant to memory degradation. Most authentication errors were not due to users forgetting their password, but were due to execution friction - that is, performing a poorly calculated directional mapping in a dynamic environment.

Although Systems A and B incur an increased penalty in misclicks due to the mental rotation process, this error distribution is an acceptable compromise for users prioritizing maximum resistance against shoulder-surfing attacks [8]. On the other hand, the most mechanically stable models (System C and D) are the most cognitively and physically least strained in terms of misclicks.

6.2.5 Demo Phase Analysis: Initial User Onboarding

All the participants had to pass through a Demo Phase before the formal memory and efficiency tests. The sandboxed environment was used to give the users time to become acquainted with the logic of the GridLock authentication process, without the stress of a documented memory test. The performance logs of this first onboarding stage (200 attempts to unlock Compass Lock and 222 attempts to unlock Compass Pro) provide important insights into the Initial Learning Friction and the direct effect of system demonstrations on user flexibility.

6.2.5.1 Initial Success Rate and the "Aha! Moment"

The most important measure at the onboarding stage is the speed with which a user learns the logic of the system. To measure this, the success of the first three consecutive endeavours in the demo setting were examined.

The success rate progression during the demo phase is shown in Figure 6.2.5.1: Success Rate Progression During Demo Phase below:

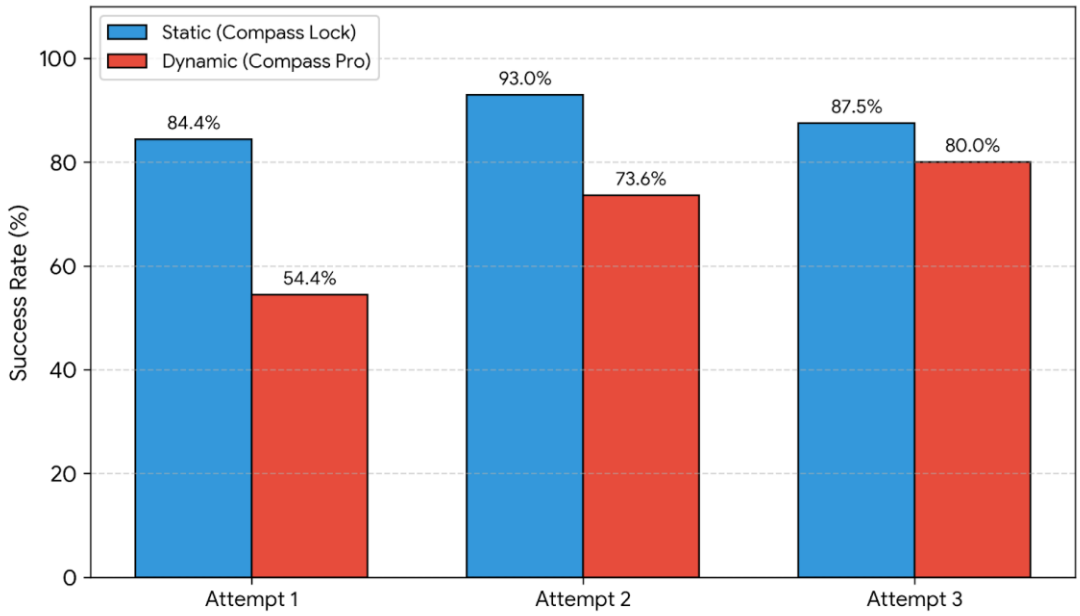


Figure6.2.5.1 Success Rate Progression During Demo Phase

As it is shown in Figure 6.2.5.1, the information demonstrates an evident deviation in first intuition:

- High Intuition in Static Models: In the case of the Static Compass Lock system, participants had a very high rate of success on their first attempt; a success rate of 84.4%. This had gone up to 93.0 by the second attempt. This means that the fixed-north rationale is very intuitive and only demands almost no education to get the average user to follow.

- The Dynamic Learning Curve: On the contrary, the Dynamic Compass Pro system presented a more challenging initial challenge. The initial attempt was able to achieve a low success rate of 54.4%, which highlights the initial cognitive shock of the mental rotation necessity. But on Attempt 3, the success rate shot up to 80.0%. Such a 25 percent or more improvement in only three tries is the Aha! of the users. Moment- the exact moment when they grasped the logic of dynamic rotation. This rapid cognitive adaptation aligns with the human-cognitive perspectives observed in recognition-based graphical authentication [20].

6.2.5.2 Speed Adaptation and Onboarding Friction

Besides accuracy, the time in which each demo attempt was completed was also recorded to gauge the speed at which users could adjust the speed of their execution.

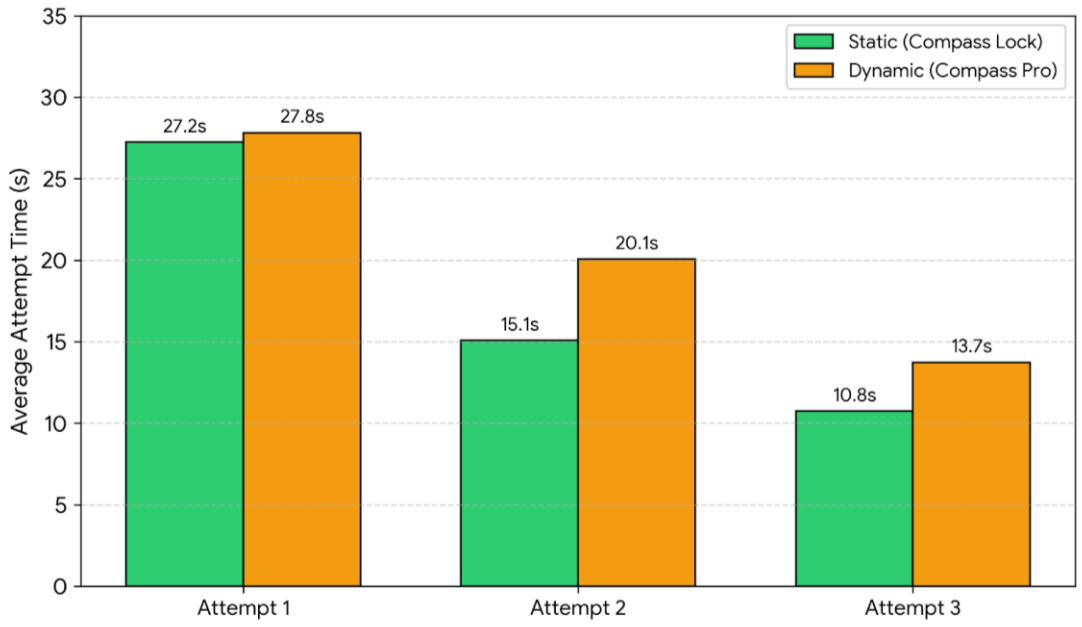


Figure 6.2.5.2 Speed Progression During Demo Phase

Figure 6.2.5.2.2 shows a violent decrease in operation time in the demo stage:

- First Attempt Caution: In Attempt 1, it was found that both systems took a long time to execute (27.2s for Static, 27.8s for Dynamic). Consistent with studies on image grid visualizations [11], this was not surprising because users were carefully going through the graphical interface, finding objects, and validating their inputs.

- Rapid Speed Optimization: By Attempt 3, the Static system execution time had reduced by more than 60% to only 10.8s. The Dynamic system also experienced a drastic decrease, decreasing to 13.7s.

- Conclusion: The sharp negative slope of the attempt times confirms the fact that the graphical interface is extremely convenient to use in the system. When the rationality behind it is known, the execution speed becomes automatic, needing no long tutorials to get it to go.

6.2.5.3 Summary of Demo Impact

The evaluation of the Demo Phase makes it clear that although the GridLock system (and its dynamic variants in particular) presents a new model of authentication, the onboarding friction is very short. The first cognitive barrier can be surmounted by the user in 2 to 3 practice attempts, which is a critical success factor in standard usability evaluations for graphical passwords [31].

This result is extremely beneficial for real-world deployment. It indicates that a brief interactive tutorial, taking less than a minute of a user's time, is sufficient to transform a completely novice user into a capable operator. As emphasized in literature regarding the overarching goals of graphical passwords [9], this rapid onboarding effectively balances the complex security mechanisms discussed in Section 6.2.2 with the long-term expert performance established in Section 6.2.3.

6.2.6 Impact of Password Complexity (Object Count) on Efficiency

In this section, the impact of the complexity of the password (the number of objects (4, 5, or 6)) on the efficiency of registration and authentication is discussed. This relationship is essential in deciding the best balance between the security (longer passwords) and the usability (faster set up and login).

6.2.6.1 Password Creation (Registration) Efficiency

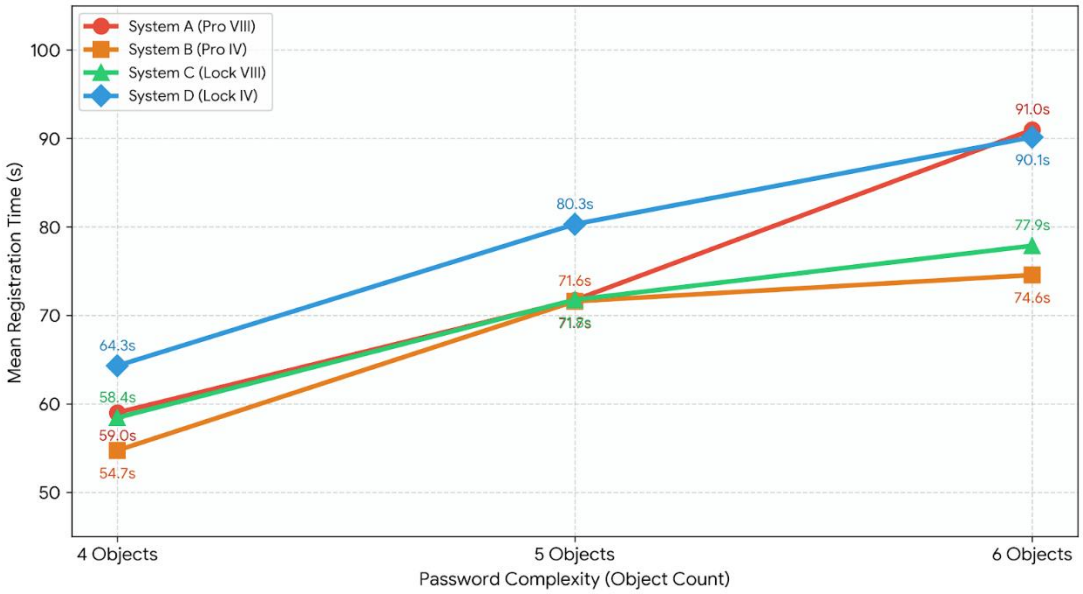


Figure 6.2.6.1 Correlation between Object Count and Creation Time

The time taken to generate a password, according to Figure 6.2.6.1, is directly proportional to the number of objects picked. This linear pattern is similar in all the four prototypes.

- Linear Growth: The average time to add one object into the password sequence is around 12-15 seconds. This time frame is comprised of the time the user requires in the process of choosing a new object [20], the time the user spends on the randomized compass (Pro models), and the time the user spends in assuring directional mapping.

- System D Anomaly: In line with the results of Section 6.2.1.1, System D registered the largest time of all the objects. This also adds into the Priming Effect, with users taking longer to move about the interface on the initial interaction (in this case System D with most participants) with or without that password length.

6.2.6.2 Authentication (Login) Efficiency and Cognitive Load

Registration is a one time operation whereas authentication time identifies the viability of the system on a daily basis. To measure this properly, the average length of time to log in was calculated in terms of the number of actual objects as was set by the users. In the particular examination, the data of controlled memory tests and penetration test were totally disregarded to capture pure and actual user behaviors in the real world.

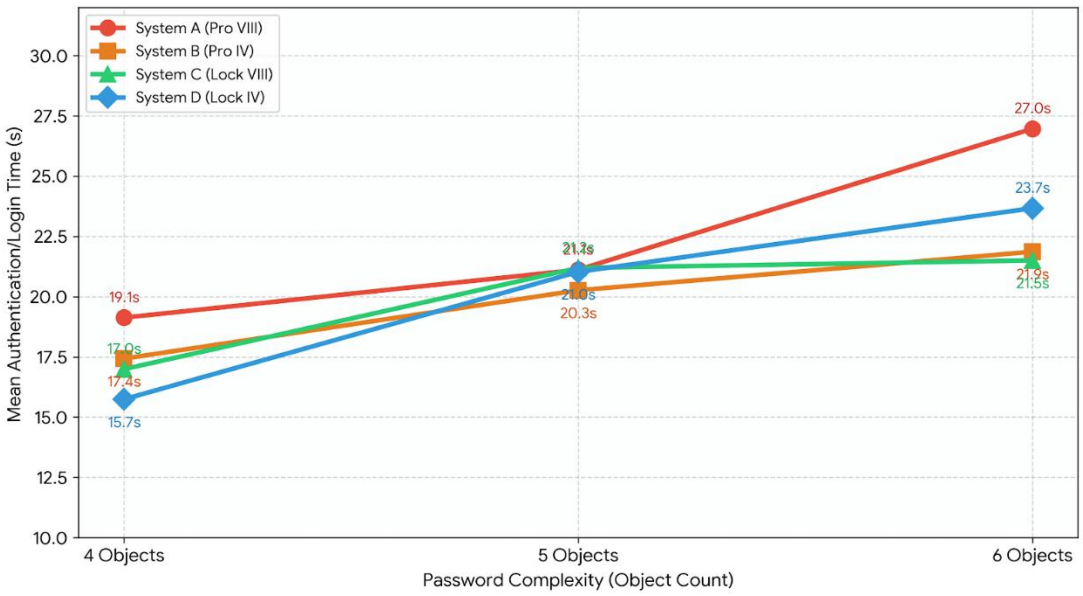


Figure 6.2.6.2 Impact of Password Length on Authentication Time

The dependence between password length and authentication speed as shown in Figure 6.2.6.2 indicates the unique cognitive scaling characteristics of the four prototypes:

- The Linear Growth Phase (4 to 5 Objects): The transition from 4 to 5 objects introduces a noticeable but manageable time penalty. Across all four prototypes, authentication time slowed by an average of 3 to 5 seconds (e.g., System D slowed to 21.0s compared to 15.7s). This aligns with established human-cognitive perspectives [20], as scanning, recognizing, and processing one extra visual object within a grid inherently requires a predictable amount of mental processing time.

- The Cognitive Bottleneck (The 6-Object Mark): But a growth in the password to 6 objects produced a divergent effect on performance based on the type of system.
  - In the cases of the static and 4-directional systems (Systems B, C and D) the time increment was less and it settled between 21.5s to 23.6s.
  - On the other hand, the most complicated dynamic prototype, System A (Pro VIII) found its performance reduced drastically to almost 27.0 seconds.

- Psychological Implication: The phenomenon is an ideal representation of the limit of the working memory in humans. This aligns perfectly with contemporary cognitive psychology, which establishes that the core working memory capacity for processing complex dynamic variables is strictly limited to 3 to 5 chunks [37]. Although the user can easily handle 5 Object + Direction pairs, it becomes difficult to handle 6 dynamic variables on an 8-way rotating compass that requires the user to focus on 6 items at the same time. Users often hesitated and performed extra verification of their mental rotations to prevent misclicks, which was the cause of the drastic execution delay.

6.2.6.3 Design Recommendation: The "Sweet Spot"

By combining the results of both registration and filtered authentication efficiency, this paper can come up with a conclusion that 5 Objects is the best configuration of the GridLock system.

Several objects (5) give the system a very high security entropy (exponentially harder to shoulder-surf than 4 objects) and maintain the daily login rate at a very acceptable 20 to 21-second range across all prototypes. Above all, the 5-object password limit can spare users of the extreme cognitive bottleneck and time penalties at 6 objects of dynamic systems.

6.3 Project Challenges

The development, implementation and analysis of the GridLock system had a number of major challenges. It was important to overcome these challenges to ascertain the validity of the empirical evidence and the achievement of the research objectives.

6.3.1 Technical Implementation of Dynamic Mental Rotation

The design of the dynamic logic of System A (Pro VIII) and System B (Pro IV) was one of the main developmental issues.

- State Synchronization: The Compass Pro variants (in contrast to fixed-point graphical passwords) also required that the system state dynamically refresh a randomized indicator of North, every time authentication is performed. It was technically challenging to have smooth simultaneous rotation of the displayed compass and the unseen logical coordinate map without resulting in lag in the user interface (UI).

- Precision Constraints: The 8-directional logic (System A and C) meant that the grid interaction areas needed to be divided into 45 degree segments. The hitboxes needed to be calibrated to record touch inputs without error (reducing technical fat-finger misclicks) and yet be sensitive enough to record the direction desired by the user, taking the refinement of the UI through several iterations.

6.3.2 Execution of the Longitudinal User Study

The behavioural and logistical difficulties involved in conducting a 7-day continuous memory retention test (Objective 3) were a major challenge in terms of managing the participants.

- Participant Fatigue and Retention: The daily logging in over a week caused some testing fatigue, especially among the participants under the cognitive heavy System A; they needed repeated follow ups and explicit explanation of the testing procedures so as to remain motivated to go through the testing plateau (Days 1 to 3).

- Assuring Test Integrity: The memory test was intended to assess mental mapping. One of the biggest issues was to make sure that participants did not write down their passwords with a pencil or make a screenshot during the registration stage. This was alleviated by performing the first setup under observation and expressly asking the users to solely depend on their spatial memory.

6.3.3 Data Cleansing and Analytical Complexity

The user testing stage produced a huge amount of data of more than 1,500 raw authentication logs. This data was very complex to process to give meaningful HCI (Human-Computer Interaction) insights.

- Isolating Variables: The raw database initially mixed information of the Demo Phase with the Penetration Test and the actual Memory Test. In order to isolate the pure naturalistic user data, as shown in Section 6.2.4 and 6.2.6, stringent data filtering was necessary. Clearly, the omission of the penetration test data would have indeed overstated the failure rates and skewed the usability results.

- Categorizing Intent of the error: It was hard to distinguish between a mechanical error (e.g. clicking too fast) and a cognitive error (e.g. miscalculating the mental rotation) using the numerical logs only. This necessitated matching the Total Misclicks measure to the Failed Sessions measure in order to effectively infer user behavior.

6.3.4 Balancing the Usability-Security Trade-off

The deepest conceptual problem of the project was, to come up with a system which meets the two sides of the spectrum: complete security against shoulder-surfing and realistic everyday usability.

- Since the penetration testing (Section 6.2.2) required high complexity (randomized rotation), it automatically impaired the initial learning curve (Section 6.2.5). Fine-tuning the system to discover the "Sweet Spot" which turned out to be the 5-object sequence in Section 6.2.6 involved a tradeoff that had to be constant between mathematical entropy and human cognitive abilities.

6.4 Objectives Evaluation

The final evaluation of the success of this project will be based on the extent to which the empirical results respond to the initial research questions that were set at the inception of the research. This section will be a summative analysis of each of the objectives in accordance with the data and understanding acquired throughout the testing stages.

6.4.1 Evaluation of Objective 1: Usability and Efficiency

The objective of the evaluation is to assess the objective of the evaluation that is Objective 1: Usability and Efficiency.

Objective: To evaluate the usability of dynamic grid layouts with directional authentication-based graphical password prototypes by analysing registration time, login time, and success rate.

Evaluation: This objective was met. The system was extremely accessible, and users with a learning friction of only 2 to 3 attempts were able to overcome this obstacle as described in the Demo Phase Analysis (Section 6.2.5). Moreover, the analysis of usability (Section 6.2.6) revealed that the most effective password configuration is 5-object password setup, which is the so-called sweet spot. With this level of complexity, the system has a fair registration time (around 70 seconds) and an extremely fast daily authentication rate (around 1821 seconds in average) across all prototypes. The system proved to be well operationally viable despite the implementation of a new mental rotation mechanic.

6.4.2 Evaluation of Objective 2: Resistance to Shoulder-Surfing

Objective: To assess the security against shoulder-surfing attacks through controlled observation tests, investigating the effectiveness of the directional mechanism in resisting cracking attempts.

Evaluation: This objective was surpassed. The penetration test described in Section 6.2.2 gave conclusive evidence on the defensive strength of the system. In 378 attempts at the attacks that observers recorded, the success rate stood at the absolute zero of 0.00. Most remarkably, the GridLock system maintained this ideally resistant behavior despite the public release of the underlying directional mapping logic to the attackers. It demonstrates that the cognitive difficulty of following dynamic pairs of "Object + Direction" is a successful way of generating an insurmountable observation gap and effectively counteracting the threat of shoulder-surfing.

6.4.3 Evaluation of Objective 3: Learnability and Long-Term Memorability

Objective: To analyze long-term recall by conducting a 7-day longitudinal study, determining changes in login performance and error patterns to establish user memorability trends.

Evaluation: This Objective was met. A positive and concise learning curve was charted by the 7-day longitudinal memory study (Section 6.2.3). By Day 4, all participants (irrespective of the prototype they were placed in) had achieved the "Cognitive Plateau" by converting conscious calculation to muscle memory quickness. As of Day 7, users were able to reach expert-level success (>80 percent). In addition, the detailed error analysis (Section 6.2.4) proved that the fundamental object-recognition part of the system is extremely stable, and it is the friction of execution (misclicks) that leads to failures, as opposed to the real loss of memory. This confirms the fact that the GridLock logic is highly memorable and can be retained in the long term.

6.4.4 General Conclusion of the Evaluation.

In short, the GridLock project was able to manoeuvre the tricky usability-security trade-off. The project not only achieved but strictly tested all its original research goals by converting the abstract spatial directions and image recognition into an integrated authentication logic using a large amount of empirical data.

6.5 Concluding Remark

In Conclusion, the overall testing and assessment of the GridLock system have achieved solid empirical indicators that validate the main principles of system design. The system was subjected to a set of intensive usability tests, longitudinal memory tests, and systematic penetration tests, and it was shown to have an unprecedented capability to fully counteract observation-based (shoulder-surfing) attacks. The physical input-physical secret decoupling of the authentication secret was very effective, with a zero-percent breach rate when full logic disclosure was present.

Although introducing dynamic mental rotation provided an apparent cognitive obstacle at first, empirical evidence supported the idea that users quickly reduced this onboarding resistance. Based on the stability of the Picture Superiority Effect, participants were able to switch to the process of deliberate logical reasoning to muscle memory. The fact that the cognitive plateau was achieved within four days confirms that the logic of space and direction is most learnable, and fully appropriate to be retained over time.

Additionally, the stepwise examination of password complexity determined the 5-object sequence as the ultimate working sweet spot. This design is effective in eliminating the overall usability-security trade-off, with users insulated against cognitive bottlenecks without compromising high theoretical entropy or the most efficient daily login rate.

After critically examining the performance measures, behavioral patterns of error and successful attainment of all the research objectives, this chapter ends the evaluation section of the study. Chapter 7, the following and the last chapter, will generalize these findings into a project conclusion, and describe the scholarly and practical contributions of this study and suggest possible ways to improve on it.

CHAPTER 7

Conclusion and Recommendation

7.1 Conclusion

The omnipresence of mobile devices has rendered observation-based attacks, especially shoulder-surfing, a critical menace to conventional authentication schemes like PINs and even static pattern lockouts. In a move to reverse this fatal weakness, the present project was able to conceptualize, develop, and test GridLock, a new recognition-based graphical password system, which incorporates spatial-directional logic and dynamic mental rotation.

The system was shown to be very effective after a 7-day longitudinal usability test and a 7-day structured penetration test, which was conducted through rigorous empirical testing. Most significantly, GridLock also obtained a 100 percent resistance to shoulder-surfing. In 378 direct observation attempts, including when the underlying authentication logic was revealed directly to attackers, the system was not broken. This conclusively demonstrates that the physical interaction (the grid click) and the cognitive secret (the Object + Direction mapping) can be decoupled to produce an unbridgeable gap in observation to adversaries.

In terms of usability and learnability, the project taken into consideration and addressed the usability-security trade-off that is intrinsic to usability. Although the dynamic mental rotation mechanic caused some initial cognitive friction, empirical evidence showed that users quickly became accustomed to it. Using the deep permanence of the Picture Superiority Effect, participants shifted the conscious calculation to procedural muscle memory, which they could reliably use to reach a cognitive plateau in only four days of practice. Moreover, the experiment was capable of finding 5-object sequence as the operational sweet spot, which offers strong mathematical entropy and yet offers very efficient daily login rates (average 20 seconds).

Overall, the GridLock system was able to fulfill all of the set research goals. It demonstrates that a very safe, observation-resistant graphical authentication scheme can be effectively employed without irreversibly estranging users. Being able to turn cognitive spatial tasks into a daily routine making it more intuitive, GridLock can be viewed as a highly viable and innovative alternative to the old paradigm of authentication.

7.2 Future Work Recommendations.

Although the conceptual and operational feasibility of the GridLock system has been validated, multiple opportunities to improve the system in the future have been outlined to make the system commercially ready and more widely explored by academia:

1. Resilience Assessment vs AI-Aided Recording Attacks:

Although this research found that the resistance to real-time human observation and shoulder-surfing was 100 percent, the threat environment is still dynamic. Future research must examine how well the system is resistant to more complex, automated attacks, including high-frame-rate video recording with Computer Vision and Machine Learning algorithms. Assessing the ability of AI to infer the latent Object + Direction rationale by jointly analyzing several sessions of recorded authentication will play a crucial role in securing the GridLock system against future cyber threats.

2. Long-term memory decay testing:

In this project, short-term learnability and memorability was proven by a 7-day longitudinal study. Nevertheless, a future study ought to carry out longer studies (e.g., 30-day or 60-day periods) to test memory decays. The research to determine whether the users are still able to accurately recall their complex spatial-directional mapping of the system after a long inactivity will further prove the reliability of the system in the long run.

3. Visual Object Pool personalization:

To further streamline the onboarding process and decrease the initial cognitive load, the next round must enable users to define their visual object pools. Rather than using the standard icons provided by the system, to enable customization, it would be of great relevance to enable users to add their own images (e.g. photos of relatives, pets, or other common points of interest). The impact of the deep psychological familiarity and emotional attachment to personalized pictures on long-term memorability and authentication speed would be a nice addition to the existing HCI assessment.

4. Integration as Multi-Factor Authentication (MFA) Component:

Instead of being a primary password by itself, GridLock can be used to a tremendous effect as a sophisticated secondary security measure in high-security applications (e.g., mobile banking or enterprise system data access). As the next step, it may contemplate a smooth combination of GridLock and biometric authentication (either FaceID or fingerprint scanning) to offer an ultimate defense mechanism that will involve both physical presence and cognitive verification

REFERENCES

[1] P. Ray, R. Mukherjee, D. Giri, and M. Sasmal, “SmartGP: a framework for a Two-Factor graphical password authentication using smart devices,” in Lecture notes in networks and systems, 2023, pp. 231–240. doi: 10.1007/978-981-99-2680-0_21.

[2] P. Ray, D. Giri, W. Meng, and S. Hore, “GPOD: An efficient and secure graphical password authentication system by fast object detection,” Multimedia Tools and Applications, vol. 83, no. 19, pp. 56569–56618, Dec. 2023, doi: 10.1007/s11042-023-17571-4.

[3] A. P. Zuha, A. Joshi, S. Deshpande, A. Mohalik, R. Naik, and V. Banahatti, “Graphical Passwords for Emergent Users: A Four-Day Recall Comparative Study on PIN, Passfaces and Celebrities,” in Studies in computational intelligence, 2024, pp. 75–97. doi: 10.1007/978-981-97-4335-3_4.

[4] X. Chu, H. Sun, and Z. Chen, “PassPage: Graphical password authentication scheme based on web browsing records,” in Lecture notes in computer science, 2020, pp. 166–176. doi: 10.1007/978-3-030-54455-3_12.

[5] M. N. Al-Ameen, K. Fatema, M. K. Wright, and S. Scielzo, “The impact of cues and user interaction on the memorability of System-Assigned Recognition-Based graphical passwords,” Symposium on Usable Privacy and Security, pp. 185–196, Jan. 2015, [Online].Available:https://www.usenix.org/system/files/conference/soups2015/soups15-paper-al-ameen.pdf

[6] T. Khodadadi, Y. Javadianasl, F. Rabiei, M. Alizadeh, M. Zamani, and S. S. Chaeikar, “A Novel Graphical Password Authentication Scheme with Improved Usability,” In 2021 4th International Symposium on Advanced Electrical and Communication Technologies, pp. 01–04, Dec. 2021, doi: 10.1109/isaect53699.2021.9668599.

[7] A. H. Shnain and S. H. Shaheed, “The use of graphical password to improve authentication problems in e-commerce,” AIP Conference Proceedings, vol. 2016, p. 020133, Jan. 2018, doi: 10.1063/1.5055535.

[8] N. I. Dias, M. S. Kumaresan, and R. S. Rajakumari, “Deep learning based graphical password authentication approach against shoulder-surfing attacks,” Multiagent and Grid Systems, vol. 19, no. 1, pp. 99–115, Jun. 2023, doi: 10.3233/mgs-230024.

[9] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin, and G. R. Alavalapati, “Graphical passwords: Behind the attainment of goals,” Security and Privacy, vol. 3, no. 6, Jul. 2020, doi: 10.1002/spy2.125.

[10] Z. Li, C. Xi, Q. Zhang, and X. Zheng, “A graphical authentication system controlled by eye movement,” IOP Conference Series Materials Science and Engineering, vol. 428, p. 012002, Oct. 2018, doi: 10.1088/1757-899x/428/1/012002.

[11] C. Katsini, G. E. Raptis, C. Fidas, and N. Avouris, “Does image grid visualization affect password strength and creation time in graphical authentication?,” In Proceedings of the 2018 International Conference on Advanced Visual Interfaces, pp. 1–5, May 2018, doi: 10.1145/3206505.3206546.

[12] B. O. ALSaleem and A. I. Alshoshan, “Multi-Factor Authentication to Systems Login,” In 2021 National Computing Colleges Conference (NCCC), pp. 1–4, Mar. 2021, doi: 10.1109/nccc49330.2021.9428806.

[13] P. Jittibumrungrak and N. Hongwarittorrn, “A Preliminary Study to Evaluate Graphical Passwords for Older Adults,” In Proceedings of the 5th International ACM in-Cooperation HCI and UX Conference, pp. 88–95, Apr. 2019, doi: 10.1145/3328243.3328255.

[14] A. F. Rasheed, M. Zarkoosh, and F. R. Elia, “Enhancing graphical password authentication system with deep learning-based arabic digit recognition,” International Journal of Information Technology, vol. 16, no. 3, pp. 1419–1427, Oct. 2023, doi: 10.1007/s41870-023-01561-8.

[15] K. Anjitha and I. K. Rijin, “Captcha as graphical passwords-enhanced with video-based captcha for secure services,” In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 213–217, Oct. 2015, doi: 10.1109/icatcct.2015.7456884.

[16] H. M. Aljahdali and R. Poet, “Educated Guessing Attacks on Culturally Familiar Graphical Passwords Using Personal Information on Social Networks,” In Proceedings of the 7th International Conference on Security of Information and Networks, pp. 272–278, Sep. 2014, doi: 10.1145/2659651.2659727.

[17] W.-C. Ku, Y.-C. Yeh, B.-R. Cheng, and C.-J. Chang, “A Sector-Based Graphical Password Scheme with Resistance to Login-Recording Attacks,” IEICE Transactions on Information and Systems, vol. E98.D, no. 4, pp. 894–901, Jan. 2015, doi: 10.1587/transinf.2014edp7302.

[18] V. Rajanna, S. Polsley, P. Taele, and T. Hammond, “A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks,” In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1978–1986, May 2017, doi: 10.1145/3027063.3053070.

[19] E. Abusham, B. Ibrahim, K. Zia, and S. A. Maskari, “An Integration of New Digital Image Scrambling Technique on PCA-Based Face Recognition System,” Scientific Programming, vol. 2022, pp. 1–17, Nov. 2022, doi: 10.1155/2022/2628885.

[20] C. Katsini, C. Fidas, M. Belk, G. Samaras, and N. Avouris, “A Human-Cognitive perspective of users’ password choices in Recognition-Based graphical authentication,” International Journal of Human-Computer Interaction, vol. 35, no. 19, pp. 1800–1812, Feb. 2019, doi: 10.1080/10447318.2019.1574057.

[21] A. Constantinides, M. Belk, C. Fidas, and G. Samaras, “On Cultural-centered Graphical Passwords,” In Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization, pp. 245–249, Jul. 2018, doi: 10.1145/3209219.3209254.

[22] S. Z. Nizamani, S. R. Hassan, R. A. Shaikh, S. T. Bakhsh, and MIR Labs, “An evaluation model for recognition-based graphical password schemes,” 2019. [Online]. Available: https://www.mirlabs.org/jias/secured/Volume14-Issue3/Paper7.pdf

[23] H. Assal, A. Imran, and S. Chiasson, “An exploration of graphical password authentication for children,” International Journal of Child-Computer Interaction, vol. 18, pp. 37–46, Jul. 2018, doi: 10.1016/j.ijcci.2018.06.003.

[24] M. A. Mohamed, “The effects of culture on authentication Cognitive Dimensions,” in Advances in intelligent systems and computing, 2019, pp. 37–42. doi: 10.1007/978-3-030-11051-2_6.

[25] W.-C. KU, B.-R. CHENG, Y.-C. YEH, and C.-J. CHANG, “A Simple Sector-Based Textual-Graphical Password Scheme with Resistance to Login-Recording Attacks,” *IEICE Transactions on Information and Systems*, vol. E99.D, no. 2, pp. 529–532, Jan. 2016, doi: https://doi.org/10.1587/transinf.2015edl8080.

[26] Dhanush kumar Ratakonda, Hoda Mehrpouyan, and J. A. Fails, “‘Pictures are easier to remember than spellings!’: Designing and evaluating KidsPic — A graphical image-based authentication mechanism,” *International Journal of Child-Computer Interaction*, vol. 33, pp. 100515–100515, Jul. 2022, doi: https://doi.org/10.1016/j.ijcci.2022.100515.

[27] I. Sharma and A. Joshi, “To Shuffle or Not to Shuffle: Evaluation of the Effect of Shuffling on Celebrity Passfaces,” *Communications in computer and information science*, pp. 26–50, Jan. 2025, doi: https://doi.org/10.1007/978-3-031-80829-6_2.

[28] H. Sun, K. Wang, X. Li, N. Qin, and Z. Chen, "PassApp," *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pp. 306–315, Aug. 2015, doi: https://doi.org/10.1145/2785830.2785880.

[29] S. Azad *et al.*, "VAP code: A secure graphical password for smart devices," *Computers & Electrical Engineering*, vol. 59, pp. 99–109, Apr. 2017, doi: https://doi.org/10.1016/j.compeleceng.2016.12.007.

[30] M. Harshini, P. L. Sai, S. Chennamma, Thanuja, A. G. Reddy, and H. S. Kim, "Easy-Auth: Graphical Password Authentication using a Randomization Method," *IEEE Xplore*, Nov. 01, 2021. https://ieeexplore.ieee.org/document/9647825 (accessed Sep. 07, 2023).

[31] H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Graphical One-Time Password (GOTPass): A usability evaluation," *Information Security Journal: A Global Perspective*, vol. 25, no. 1–3, pp. 94–108, Apr. 2016, doi: https://doi.org/10.1080/19393555.2016.1179374.

[32] J. P, "Towards Usability Evaluation of Jumbled PassSteps," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 4, pp. 1032–1037, Aug. 2019, doi: https://doi.org/10.30534/ijatcse/2019/08842019.

[33] S. Lavanya, N. M. SaravanaKumar, V. Vijayakumar, and S. Thilagam, "Secured Key Management Scheme for Multicast Network Using Graphical Password," *Mobile Networks and Applications*, vol. 24, no. 4, pp. 1152–1159, May 2019, doi: https://doi.org/10.1007/s11036-019-01252-4.

[34] A. Constantinides, M. Belk, Christos Fidas, and A. Pitsillides, "On the Accuracy of Eye Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords," pp. 201–205, Jun. 2019, doi: https://doi.org/10.1145/3320435.3320474.

[35] A. Constantinides, Christos Fidas, M. Belk, and A. Pitsillides, "On the Personalization of Image Content in Graphical Passwords based on Users' Sociocultural Experiences," Jun. 2019, doi: https://doi.org/10.1145/3314183.3324966.

[36] Y. L. Ho, S. H. Lau, and A. Azman, "Picture superiority effect in authentication systems for the blind and visually impaired on a smartphone platform," *Universal Access in the Information Society*, Oct. 2022, doi: https://doi.org/10.1007/s10209-022-00928-1.

[37] N. Cowan, “The many faces of working memory and short-term storage,” *Psychonomic Bulletin & Review*, vol. 24, no. 4, pp. 1158–1170, Nov. 2017, doi: https://doi.org/10.3758/s13423-016-1191-6.

APPENDIX A

Raw Data Snippets and Dataset Overview

1. User Information Dataset

	User ID	Name	Email	Age	Gender	Contact Phone	Agreed To Terms
2	0suGsZcE6kaN81A0tyvNDOqHtnr2	P01	P01_01@gmail.com	24	Male	ANONYMIZED	Yes
3	1eotTEtMaeQ7ce8D71DfW5zv4sf2	P02	vivianlau003@gmail.com	22	Female	ANONYMIZED	Yes
4	1ih3PIHbBAbwp5fVvdWM7KtGy3J3	P03	P03_2004@gmail.com	21	Female	ANONYMIZED	Yes
5	2Xktl6ZtYFdM5GJo3AxdL0B6h4N2	P04	P04_03@gmail.com	22	Male	ANONYMIZED	Yes
6	2pmyPlC5NnaPondS5gGOv9xqWaB3	P05	P05_2005@gmail.com	20	Female	ANONYMIZED	Yes
7	3YPFTAjel1S4ysf4kiJ4BayDlRU2	P06	P06_02@gmail.com	23	Female	ANONYMIZED	Yes
8	4e78s4cndFWN0ufQ2pPFQcWXjit2	P07	P07_5566@gmail.com	24	Male	ANONYMIZED	Yes
9	4gIGIlEjZKNmE5l8QVeDVSY41MX2	P08	P08_01@gmail.com	24	Female	ANONYMIZED	Yes
10	57eUA5HX2TMEFl7KKujCVAsJ2cQ2	P09	P09_04@gmail.com	21	Female	ANONYMIZED	Yes
11	5g7pQ6m0nBclrM2NzWce8NAjB5K2	P10	P10_00@gmail.com	24	Male	ANONYMIZED	Yes
12	5yPUxJz7kyclo3SavPpJ7q52p4s2	P11	P11_i2004@gmail.com	22	Male	ANONYMIZED	Yes
13	6TSYtWlgygPpCukzjzHBtgFXCO03	P12	P12_003@gmail.vom	22	Male	ANONYMIZED	Yes
14	6VqG629ORGbExVsz3sGcu73gd5m1	P13	P13_1@utar.my	22	Male	ANONYMIZED	Yes
15	7VjafaZes0PPC90RTZuqEa6zl5e2	P14	P14_7227@gmail.com	24	Female	ANONYMIZED	Yes
16	7dkd6H2mFfQy3O1mOZobpkSUvgC2	P15	P15_0325@gmail.com	23	Male	ANONYMIZED	Yes
17	8V6nNaDjyBfhBOudYkH7Dz7XwDv1	P16	P16_0125@gmail.com	23	Male	ANONYMIZED	Yes
18	8Vc1yx0kitYNcEJ4aTQ0FSXJOpu1	P17	P17_03@gmail.com	22	Male	ANONYMIZED	Yes
19	94HxioPsWZcGyoAGBb0k7XCp7m22	P18	P18_2003@gmail.com	22	Male	ANONYMIZED	Yes
20	967OdGAJSBa4cBJmzKlfbXJPadG2	P19	P19_007@gmail.com	18	Female	ANONYMIZED	Yes
21	AiI3lmO3zuPEFzr8CVOA3rpmAVR2	P20	P20_03@gmail.com	22	Male	ANONYMIZED	Yes
22	B2ecuRcQZ1dlmw1PXe47EJsM4nx1	P21	P21_06@gmail.com	20	Male	ANONYMIZED	Yes
23	B8KyXTldmgOjM5VLmHdUdszaP7Q2	P22	P22_01@gmail.com	24	Male	ANONYMIZED	Yes
24	BLI1w9YujRYsq7yGKyxl33j5KLI3	P23	P23_03@gmail.com	22	Male	ANONYMIZED	Yes
25	Bwm1JHBVdycou5PfnRg9aUVS5x73	P24	P24_05@gmail.com	20	Male	ANONYMIZED	Yes

2. Usability Test Dataset

	User Name	User ID	Summary ID	Password Name	Session Timestamp	Test Number	Success	Skipped	Login Time (ms)	Login Time (s)	Object Name	Expected Direction
2	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	1	FALSE	FALSE	27495	27.495	System D	N,E,N,E
3	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	2	TRUE	FALSE	13672	13.672	System D	N,E,N,E
4	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	3	TRUE	FALSE	17559	17.559	System D	N,E,N,E
5	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	4	FALSE	FALSE	15904	15.904	System D	N,E,N,E
6	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	5	TRUE	FALSE	14246	14.246	System D	N,E,N,E
7	P01	ItRECEe0MgXwumH	OgQfAqwqjseUBQldyd6g	System D	2026-03-22 04:48:55	6	TRUE	FALSE	17958	17.958	System D	N,E,N,E
8	P01	ItRECEe0MgXwumH	MptyKdqkKPFIp3vNgSPt	System D	2026-03-22 04:48:52	6	TRUE	FALSE	17958	17.958	System D	N,E,N,E
9	P01	ItRECEe0MgXwumH	sl0Z4t5FMOuElClPKsOc	System D	2026-03-22 04:48:32	5	TRUE	FALSE	14246	14.246	System D	N,E,N,E
10	P01	ItRECEe0MgXwumH	zZw3sP4ujOw3JPK7RFMF	System D	2026-03-22 04:48:16	4	FALSE	FALSE	15904	15.904	System D	N,E,N,E
11	P01	ItRECEe0MgXwumH	wm25YneeRN05Hoq8B3eR	System D	2026-03-22 04:47:58	3	TRUE	FALSE	17559	17.559	System D	N,E,N,E
12	P01	ItRECEe0MgXwumH	JimbdPwvK2SCYyAr9DDO	System D	2026-03-22 04:47:39	2	TRUE	FALSE	13672	13.672	System D	N,E,N,E
13	P01	ItRECEe0MgXwumH	JIXG5wWjHTW0eUuVCvn2	System D	2026-03-22 04:47:23	1	FALSE	FALSE	27495	27.495	System D	N,E,N,E
14	P02	5g7pQ6m0nBclrM2N	ULSrM1H6FwiAlVgW5BmN	System D	2026-03-22 02:45:37	1	TRUE	FALSE	8708	8.708	System D	N,N,N,N
15	P02	5g7pQ6m0nBclrM2N	uMTBX7wVhNgA71Tr65dl	System D	2026-03-22 02:40:00	1	FALSE	FALSE	8922	8.922	System D	N,N,N,N
16	P03	NjlFdOcJhxMxugmrE	Ef2LzOGUGlhXu2TRNnWc	System D	2026-03-16 04:05:23	1	TRUE	FALSE	8774	8.774	System D	S,S,N,E,W
17	P03	NjlFdOcJhxMxugmrE	Ef2LzOGUGlhXu2TRNnWc	System D	2026-03-16 04:05:23	2	TRUE	FALSE	5207	5.207	System D	S,S,N,E,W
18	P03	NjlFdOcJhxMxugmrE	Ef2LzOGUGlhXu2TRNnWc	System D	2026-03-16 04:05:23	3	TRUE	FALSE	6562	6.562	System D	S,S,N,E,W
19	P03	NjlFdOcJhxMxugmrE	Ef2LzOGUGlhXu2TRNnWc	System D	2026-03-16 04:05:23	4	TRUE	FALSE	10891	10.891	System D	S,S,N,E,W
20	P03	NjlFdOcJhxMxugmrE	Ef2LzOGUGlhXu2TRNnWc	System D	2026-03-16 04:05:23	5	TRUE	FALSE	5897	5.897	System D	S,S,N,E,W

	Compass Direction	Entry Password	Compass Rotation Degrees	Formatted Entry Info	Test Timestamp	Test Date	Status	Time Category	Error Count	Error Category
2	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	FAILED	Slow (20-30s)	1	Minimal Errors (1-2)
3	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
4	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
5	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	FAILED	Moderate (10-20s)	1	Minimal Errors (1-2)
6	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
7	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
8	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
9	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
10	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:48:	2025-11-02 04	FAILED	Moderate (10-20s)	1	Minimal Errors (1-2)
11	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
12	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
13	North	gpw01/N↑;gpw06/E→;i	0	Entry: gpw01/N↑;gpw0(	2025-11-02 04:47:	2025-11-02 04	FAILED	Slow (20-30s)	1	Minimal Errors (1-2)
14	West	gpw01/S↓;gpw02/SW↙	270	Entry: gpw01/S↓;gpw02	2026-03-22 03:24:	2026-03-22 03	FAILED	Very Fast (≤5s)	4	Some Errors (3-5)
15	East	gpw01/E→;gpw02/E→;g	90	Entry: gpw01/E→;gpw02	2026-03-22 03:24:	2026-03-22 03	SUCCESS	Moderate (10-20s)	0	Perfect (No Errors)
16	North	gpw01/N↑;gpw02/N↑;	0	Entry: gpw01/N↑;gpw02	2026-03-22 02:45:	2026-03-22 02	SUCCESS	Fast (5-10s)	0	Perfect (No Errors)
17	North	gpw01/NE↗;gpw02/SW	0	Entry: gpw01/NE↗;gpw0	2026-03-22 02:40:	2026-03-22 02	FAILED	Fast (5-10s)	4	Some Errors (3-5)
18	North	gpw05/NW↖;gpw02/NI	0	Entry: gpw05/NW↖;gpw	2026-03-16 04:08:	2026-03-16 04	FAILED	Fast (5-10s)	2	Minimal Errors (1-2)
19	South	gpw05/SW↙;gpw02/SE	180	Entry: gpw05/SW↙;gpw(	2026-03-16 04:08:	2026-03-16 04	SUCCESS	Fast (5-10s)	0	Perfect (No Errors)
20	South	gpw05/SW↙;gpw02/SE	180	Entry: gpw05/SW↙;gpw(	2026-03-16 04:09:	2026-03-16 04	SUCCESS	Fast (5-10s)	0	Perfect (No Errors)

	Time Category	Error Count	Error Category	Total Objects In Sequence	Is Sequence Complete	Challenge Set	Challenge Set Size
2	Slow (20-30s)	1	Minimal Errors (1-2)	4	TRUE	gpw01;gpw06;gl	25
3	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
4	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
5	Moderate (10-20s)	1	Minimal Errors (1-2)	4	TRUE	gpw01;gpw06;gl	25
6	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
7	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
8	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
9	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
10	Moderate (10-20s)	1	Minimal Errors (1-2)	4	TRUE	gpw01;gpw06;gl	25
11	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
12	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw06;gl	25
13	Slow (20-30s)	1	Minimal Errors (1-2)	4	TRUE	gpw01;gpw06;gl	25
14	Very Fast (≤5s)	4	Some Errors (3-5)	4	TRUE	gpw01;gpw02;gl	25
15	Moderate (10-20s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw02;gl	25
16	Fast (5-10s)	0	Perfect (No Errors)	4	TRUE	gpw01;gpw02;gl	25
17	Fast (5-10s)	4	Some Errors (3-5)	4	TRUE	gpw01;gpw02;gl	25
18	Fast (5-10s)	2	Minimal Errors (1-2)	5	TRUE	gpw05;gpw02;gl	25
19	Fast (5-10s)	0	Perfect (No Errors)	5	TRUE	gpw05;gpw02;gl	25
20	Fast (5-10s)	0	Perfect (No Errors)	5	TRUE	gpw05;gpw02;gl	25

3. Penetration Test Dataset

	User Name	User ID	Password Type	Password Name	Test Date	Total Tests	Successful Tests	Failed Tests	Success Rate (%)	Average Login Time (s)	Total Session Time (s)
2	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-25 02:33:12	1	0	1	0	69.088	69
3	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 04:04:55	3	0	3	0	18.184	63
4	Penetration Test	UHFkeuodjSf	compass_pro_iv	System B	2026-02-25 02:37:57	1	0	1	0	7.657	7
5	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 18:37:33	3	0	3	0	24.87	83
6	Penetration Test	UHFkeuodjSf	compass_pro_iv	System B	2026-02-25 02:47:01	1	0	1	0	13.661	13
7	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2025-09-02 03:17:53	6	0	6	0	5.177	43
8	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-25 04:22:58	3	0	3	0	23.679	79
9	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-27 03:26:56	3	0	3	0	23.284	77
10	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-28 02:20:35	3	0	3	0	21.238	73
11	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 02:31:33	1	0	1	0	29.252	29
12	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-28 01:57:08	3	0	3	0	24.224	79
13	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 02:23:12	1	0	1	0	11.758	11
14	Penetration Test	UHFkeuodjSf	compass_lock_iv	System D	2026-02-28 02:01:35	3	0	3	0	26.418	86
15	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 02:22:46	1	0	1	0	45.072	45
16	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 02:13:59	1	0	1	0	30.307	30
17	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-25 03:17:51	3	0	3	0	23.349	77
18	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 18:30:59	3	0	3	0	23.847	80
19	Penetration Test	UHFkeuodjSf	compass_lock_iv	System D	2026-02-28 02:33:10	3	0	3	0	31.181	101
20	Penetration Test	UHFkeuodjSf	compass_pro_iv	System B	2026-02-25 18:10:56	3	0	3	0	18.884	64
21	Penetration Test	UHFkeuodjSf	compass_pro_viii	System A	2026-02-25 04:17:54	3	0	3	0	20.205	68
22	Penetration Test	UHFkeuodjSf	compass_lock_viii	System C	2026-02-25 21:25:07	3	0	3	0	19.725	71
23	Penetration Test	UHFkeuodjSf	compass_lock_iv	System D	2026-02-25 03:12:48	3	0	3	0	37.98	132
24	Penetration Test	UHFkeuodjSf	compass_pro_iv	System B	2026-02-28 02:07:45	3	0	3	0	22.125	76
25	Penetration Test	UHFkeuodjSf	compass_pro_iv	System B	2026-02-25 02:46:29	1	0	1	0	35.327	35

	me (s)	Total Session Time (s)	Fastest Login Time (s)	Slowest Login Time (s)	Median Login Time (s)	Object Count	Object Analysis	Error Analysis	Status Analysis
2	9.088	69	69.088	69.088	69.088	1		Total: 4; Avg: 4; Max: 4; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
3	8.184	63	11.562	21.965	21.026	1		Total: 10; Avg: 3.33; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
4	7.657	7	7.657	7.657	7.657	1		Total: 4; Avg: 4; Max: 4; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
5	24.87	83	17.382	28.896	28.331	1		Total: 10; Avg: 3.33; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
6	3.661	13	13.661	13.661	13.661	1		Total: 5; Avg: 5; Max: 5; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
7	5.177	43	4.573	5.523	5.216	1		Total: 25; Avg: 4.17; Max: 5; Rate: 100%	Success: 0; Failed: 6; Skipped: 0
8	3.679	79	18.528	29.477	23.031	1		Total: 15; Avg: 5; Max: 5; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
9	3.284	77	21.085	26.097	22.671	1		Total: 11; Avg: 3.67; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
10	1.238	73	13.634	35.601	14.48	1		Total: 12; Avg: 4; Max: 5; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
11	9.252	29	29.252	29.252	29.252	1		Total: 3; Avg: 3; Max: 3; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
12	4.224	79	15.472	30.444	26.757	1		Total: 11; Avg: 3.67; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
13	1.758	11	11.758	11.758	11.758	1		Total: 2; Avg: 2; Max: 2; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
14	6.418	86	7.763	35.996	35.495	1		Total: 17; Avg: 5.67; Max: 6; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
15	5.072	45	45.072	45.072	45.072	1		Total: 3; Avg: 3; Max: 3; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
16	0.307	30	30.307	30.307	30.307	1		Total: 4; Avg: 4; Max: 4; Rate: 100%	Success: 0; Failed: 1; Skipped: 0
17	3.349	77	16.976	29.499	23.571	1		Total: 13; Avg: 4.33; Max: 5; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
18	3.847	80	16.869	32.438	22.235	1		Total: 12; Avg: 4; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
19	1.181	101	27.438	33.663	32.442	1		Total: 16; Avg: 5.33; Max: 6; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
20	8.884	64	15.576	22.577	18.498	1		Total: 15; Avg: 5; Max: 5; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
21	0.205	68	13.111	28.148	19.356	1		Total: 9; Avg: 3; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
22	9.725	71	15.046	25.983	18.147	1		Total: 10; Avg: 3.33; Max: 4; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
23	37.98	132	4.253	94.496	15.191	1		Total: 17; Avg: 5.67; Max: 6; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
24	2.125	76	15.292	29.358	21.725	1		Total: 14; Avg: 4.67; Max: 5; Rate: 100%	Success: 0; Failed: 3; Skipped: 0
25	5.327	35	35.327	35.327	35.327	1		Total: 5; Avg: 5; Max: 5; Rate: 100%	Success: 0; Failed: 1; Skipped: 0

4. Memory Test Dataset

	User Name	User ID	Prototype Type	Prototype Name	Test Date	Trial Number	Is Success (1/0)	Login Time (s)	Error Count	Status	Error Category
2	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	1	1	14.295	0	SUCCESS	Perfect (No Errors)
3	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	2	0	9.891	1	FAILED	Minimal Errors (1-2)
4	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	3	1	9.29	0	SUCCESS	Perfect (No Errors)
5	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	4	1	12.422	0	SUCCESS	Perfect (No Errors)
6	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	5	1	18.103	0	SUCCESS	Perfect (No Errors)
7	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_iv	System D	2026-03-04 02:11:16	6	1	18.811	0	SUCCESS	Perfect (No Errors)
8	P02	uq5v15luopNVAzzfr1UUpRpZNo93	compass_lock_viii	System C	2026-03-04 02:12:34	1	0	17.795	3	FAILED	Some Errors (3-5)
9	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	1	1	12.399	0	SUCCESS	Perfect (No Errors)
10	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	2	1	11.008	0	SUCCESS	Perfect (No Errors)
11	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	3	1	8.92	0	SUCCESS	Perfect (No Errors)
12	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	4	0	12.271	1	FAILED	Minimal Errors (1-2)
13	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	5	1	11.49	0	SUCCESS	Perfect (No Errors)
14	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_lock_viii	System C	2026-03-04 02:13:36	6	1	9.308	0	SUCCESS	Perfect (No Errors)
15	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	1	1	18.354	0	SUCCESS	Perfect (No Errors)
16	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	2	1	14.142	0	SUCCESS	Perfect (No Errors)
17	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	3	0	12.691	1	FAILED	Minimal Errors (1-2)
18	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	4	1	12.035	0	SUCCESS	Perfect (No Errors)
19	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	5	1	10.563	0	SUCCESS	Perfect (No Errors)
20	P03	hB58SKp0O7fIyIEsUVhudboK1553	compass_lock_iv	System D	2026-03-04 02:15:08	6	1	12.93	0	SUCCESS	Perfect (No Errors)
21	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_pro_iv	System B	2026-03-04 02:16:22	1	1	20.663	0	SUCCESS	Perfect (No Errors)
22	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_pro_iv	System B	2026-03-04 02:16:22	2	1	15.79	0	SUCCESS	Perfect (No Errors)
23	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_pro_iv	System B	2026-03-04 02:16:22	3	1	16.069	0	SUCCESS	Perfect (No Errors)
24	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_pro_iv	System B	2026-03-04 02:16:22	4	1	19.123	0	SUCCESS	Perfect (No Errors)
25	P01	eAf6SLzTaNhl2KYiFMzlh3rIVhH3	compass_pro_iv	System B	2026-03-04 02:16:22	5	0	11.433	2	FAILED	Minimal Errors (1-2)

5. Demo Result Dataset

	User Name	User ID	Demo Type	Attempt Number	Success	Attempt Time (ms)	Attempt Time (seconds)	Timestamp	Demo Timestamp	User Input Sequence	Expected Sequence	User Input String
2	P01	ItRECEe0MgXwumHe7Y9c	Compass Lock	3	TRUE	13492	13.492	2026-03-22 04:45	2026-03-22 04:45:3	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
3	P01	ItRECEe0MgXwumHe7Y9c	Compass Lock	2	TRUE	11022	11.022	2026-03-22 04:45	2026-03-22 04:45:2	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
4	P01	ItRECEe0MgXwumHe7Y9c	Compass Lock	1	FALSE	31267	31.267	2026-03-22 04:45	2026-03-22 04:45:0	E;E;S	N;E;S	gpw01/E→;gpw02/E→;gpw03/S↓
5	P03	8V6nNaDjyBfhBOudYkH7(	Compass Pro	2	TRUE	37113	37.113	2026-03-05 07:43	2026-03-05 07:43:1	W;N;E	W;N;E	gpw01/W←;gpw02/N↑;gpw03/E→
6	P03	8V6nNaDjyBfhBOudYkH7(	Compass Pro	1	FALSE	34819	34.819	2026-03-05 07:42	2026-03-05 07:42:4	W;S;E	W;N;E	gpw01/W←;gpw02/S↓;gpw03/E→
7	P03	8V6nNaDjyBfhBOudYkH7(	Compass Lock	1	TRUE	20565	20.565	2026-03-05 07:37	2026-03-05 07:37:4	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
8	P04	pF2NjlXnIdZWTsUiABwJ2E	Compass Pro	1	TRUE	18014	18.014	2026-03-05 07:27	2026-03-05 07:27:5	E;S;W	N;E;S	gpw01/E→;gpw02/S↓;gpw03/W←
9	P04	pF2NjlXnIdZWTsUiABwJ2E	Compass Lock	2	TRUE	17467	17.467	2026-03-05 07:19	2026-03-05 07:19:4	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
10	P04	pF2NjlXnIdZWTsUiABwJ2E	Compass Lock	1	TRUE	25814	25.814	2026-03-05 07:19	2026-03-05 07:19:2	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
11	P05	iQNNVGfJv350R3OeksBLp	Compass Pro	2	TRUE	31463	31.463	2026-03-05 07:01	2026-03-05 07:01:5	E;S;W	E;S;W	gpw01/E→;gpw02/S↓;gpw03/W←
12	P05	iQNNVGfJv350R3OeksBLp	Compass Pro	1	FALSE	32692	32.692	2026-03-05 07:01	2026-03-05 07:01:1	E;N;W	E;S;W	gpw01/E→;gpw02/N↑;gpw03/W←
13	P05	iQNNVGfJv350R3OeksBLp	Compass Lock	2	TRUE	6087	6.087	2026-03-05 06:53	2026-03-05 06:53:2	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
14	P05	iQNNVGfJv350R3OeksBLp	Compass Lock	1	TRUE	17230	17.23	2026-03-05 06:53	2026-03-05 06:53:1	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
15	P06	B2ecuRcQZ1dlmw1PXe47	Compass Lock	2	TRUE	13735	13.735	2026-03-05 06:44	2026-03-05 06:44:4	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
16	P06	B2ecuRcQZ1dlmw1PXe47	Compass Lock	1	TRUE	20666	20.666	2026-03-05 06:44	2026-03-05 06:44:3	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
17	P07	RCWX3jIC7wPUBHfJbLJBe	Compass Pro	2	TRUE	27247	27.247	2026-03-05 05:43	2026-03-05 05:43:3	E;S;W	E;S;W	gpw01/E→;gpw02/S↓;gpw03/W←
18	P07	RCWX3jIC7wPUBHfJbLJBe	Compass Pro	1	TRUE	21229	21.229	2026-03-05 05:43	2026-03-05 05:43:0	W;N;E	W;N;E	gpw01/W←;gpw02/N↑;gpw03/E→
19	P07	RCWX3jIC7wPUBHfJbLJBe	Compass Lock	2	TRUE	9955	9.955	2026-03-05 05:29	2026-03-05 05:29:1	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
20	P07	RCWX3jIC7wPUBHfJbLJBe	Compass Lock	1	TRUE	14894	14.894	2026-03-05 05:29	2026-03-05 05:29:0	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
21	P08	CYc9inaopEVcxw1TJxWMt	Compass Pro	3	FALSE	7312	7.312	2026-03-05 05:17	2026-03-05 05:17:5	S;E;N	S;W;N	gpw01/S↓;gpw02/E→;gpw03/N↑
22	P08	CYc9inaopEVcxw1TJxWMt	Compass Pro	2	TRUE	10359	10.359	2026-03-05 05:17	2026-03-05 05:17:4	W;N;E	W;N;E	gpw01/W←;gpw02/N↑;gpw03/E→
23	P08	CYc9inaopEVcxw1TJxWMt	Compass Pro	1	TRUE	17964	17.964	2026-03-05 05:17	2026-03-05 05:17:3	E;S;W	E;S;W	gpw01/E→;gpw02/S↓;gpw03/W←
24	P08	CYc9inaopEVcxw1TJxWMt	Compass Lock	2	TRUE	13957	13.957	2026-03-05 05:09	2026-03-05 05:09:5	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓
25	P08	CYc9inaopEVcxw1TJxWMt	Compass Lock	1	TRUE	34111	34.111	2026-03-05 05:09	2026-03-05 05:09:4	N;E;S	N;E;S	gpw01/N↑;gpw02/E→;gpw03/S↓

	Expected String	Compass Rotation	Compass Direction	Compass Rotation Degree	Compass Category	Error Count	Error Positions	Accuracy (%)	Has Errors	Challenge Set	Challenge Set String	Password Object Positions	Attempt Catego
2	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw37,gpw48,gpw43,gpw05,gpw46,gpv		Success
3	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw37,gpw49,gpw43,gpw05,gpw46,gpv		Success
4	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	1		66.67	TRUE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw37,gpw49,gpw43,gpw05,gpw46,gpv	1	Error
5	gpw01/W←;gpw02/N↑;gpw03/E→	3	West	270 West (270°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw11,gpw13,gpw40,gpw30,gpw20,gpv		Success
6	gpw01/W←;gpw02/N↑;gpw03/E→	3	West	270 West (270°)		1		66.67	TRUE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw11,gpw13,gpw40,gpw30,gpw20,gpv	1	Error
7	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw10,gpw05,gpw05,gpw43,gpw09,gpv		Success
8	gpw01/E→;gpw02/S↓;gpw03/W←	1	East	90 East (90°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw37,gpw10,gpw38,gpw08,gpw06,gpv		Success
9	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw46,gpw10,gpw32,gpw30,gpw49,gpv		Success
10	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw46,gpw10,gpw32,gpw30,gpw49,gpv		Success
11	gpw01/E→;gpw02/S↓;gpw03/W←	1	East	90 East (90°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw12,gpw27,gpw33,gpw19,gpw38,gpv		Success
12	gpw01/E→;gpw02/S↓;gpw03/W←	1	East	90 East (90°)		1		66.67	TRUE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw12,gpw27,gpw33,gpw19,gpw38,gpv	1	Error
13	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw45,gpw31,gpw04,gpw18,gpw13,gpv		Success
14	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw45,gpw31,gpw04,gpw18,gpw13,gpv		Success
15	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw35,gpw40,gpw15,gpw08,gpw38,gpv		Success
16	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw35,gpw40,gpw15,gpw08,gpw38,gpv		Success
17	gpw01/E→;gpw02/S↓;gpw03/W←	1	East	90 East (90°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw05,gpw34,gpw32,gpw31,gpw50,gpv		Success
18	gpw01/W←;gpw02/N↑;gpw03/E→	3	West	270 West (270°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw05,gpw34,gpw32,gpw31,gpw50,gpv		Success
19	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw38,gpw05,gpw46,gpw43,gpw48,gpv		Success
20	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw38,gpw05,gpw46,gpw43,gpw48,gpv		Success
21	gpw01/S↓;gpw02/W←;gpw03/N↑	2	South	180 South (180°)		1		66.67	TRUE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw32,gpw29,gpw24,gpw35,gpw21,gpv	1	Error
22	gpw01/W←;gpw02/N↑;gpw03/E→	3	West	270 West (270°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw32,gpw29,gpw24,gpw35,gpw21,gpv		Success
23	gpw01/E→;gpw02/S↓;gpw03/W←	1	East	90 East (90°)		0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw32,gpw29,gpw24,gpw35,gpw21,gpv		Success
24	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw33,gpw16,gpw30,gpw14,gpw06,gpv		Success
25	gpw01/N↑;gpw02/E→;gpw03/S↓	0	North (Fixed)	0	North (Fixed) (0°)	0		100	FALSE	gpw01;gpw02;gpw03;gpw(	gpw01,gpw02,gpw03,gpw33,gpw16,gpw30,gpw14,gpw06,gpv		Success

6. Error Analysis Dataset

	User Name	User ID	Password Type	Password Name	Test Date	Total Tests	Successful Tests	Success Rate (%)	Total Errors	Average Errors per Test	Max Errors in Single Test
2	P01	N3opCLt819RhbX0BAQqXoA	compass_lock_viii	System C	2025-12-01 02:06:06	1	1	100			
3	P02	X1TaO4vwgvQYykeLXFKspZA	compass_pro_iv	System B	2025-11-03 13:08:44	1	0	0	2	2	2
4	P03	kJFOrLzEqUfK7wBfxy4AGaBS	compass_pro_iv	System B	2025-11-16 03:39:51	6	0	0	29	4.83	5
5	P03	kJFOrLzEqUfK7wBfxy4AGaBS	compass_lock_viii	System C	2025-11-16 03:37:29	1	0	0	5	5	5
6	P04	yCWNQoRJRyg23BD2eD1GA	compass_lock_iv	System D	2026-03-05 03:42:51	6	0	0	13	2.17	4
7	P05	yHTIEc27gIPBwWrQHtiGKRA	compass_pro_iv	System B	2026-03-02 09:07:32	1	0	0	6	6	6
8	P06	V7I90MEU2hTxx21geIuzMBA	compass_lock_viii	System C	2026-03-05 03:21:45	6	5	83.33	1	0.17	1
9	P07	yCWNQoRJRyg23BD2eD1GA	compass_pro_viii	System A	2026-03-05 03:52:22	1	0	0	4	4	4
10	P08	qpwhKe6POuRbaFZQHuYIwa	compass_pro_viii	System A	2026-03-05 02:59:35	1	1	100			
11	P09	IImXuTTRaNalfczyexwbDjKCI	compass_pro_viii	System A	2025-11-12 02:53:35	6	2	33.33	6	1	2
12	P10	iIBMUosMaLYRT03ZwYktjUR	compass_lock_viii	System C	2026-03-02 07:02:07	6	4	66.67	2	0.33	1
13	P11	0suGsZcE6kaN81A0tyvNDOq	compass_lock_viii	System C	2025-12-06 04:13:24	1	1	100			
14	P12	CYc9naopEVcxw1TJxWMbxx	compass_pro_iv	System B	2026-03-05 05:22:30	1	0	0	1	1	1
15	P13	UhrcQphfXhg6vi7tnBcamfvx	compass_pro_viii	System A	2025-11-03 04:13:25	1	1	100			
16	P14	xBskD2zvz1h1PoREchZBMfB	compass_lock_iv	System D	2025-12-06 04:32:57	1	1	100			
17	P15	7VjafaZes0PPC90RTZuqEa6zl	compass_lock_iv	System D	2026-03-05 07:50:29	1	0	0	4	4	4
18	P16	UHFkeuodjSfWwkPXz19g3Og	compass_lock_viii	System C	2026-02-25 02:33:12	1	0	0	4	4	4
19	P17	zqUWAKcXHua4jMDG0oO3G	compass_pro_viii	System A	2025-11-11 08:47:47	1	0	0	5	5	5
20	P18	eAf6SLzTaNhl2KYfMzlh3rIVI	compass_lock_viii	System C	2026-03-10 04:20:49	6	6	100			
21	P19	B2ecuRcQZ1dImw1PXe47EJs	compass_lock_viii	System C	2026-03-05 06:48:51	1	0	0	4	4	4
22	P20	ReYrWokDeQNIKC1boB0ZDx	compass_pro_viii	System A	2025-11-04 04:21:05	1	1	100			
23	P21	gBtGU1fOOQVAbDMfGyEbqJ	compass_lock_iv	System D	2025-11-23 07:33:40	1	1	100			
24	P22	2Xktl6ZlYFdM5GJo3AxdL0B6I	compass_lock_viii	System C	2025-12-01 01:42:53	1	0	0	1	1	1
25	P23	7VjafaZes0PPC90RTZuqEa6zl	compass_lock_viii	System C	2026-03-05 07:51:46	1	0	0	6	6	6

Min Errors in Single Test	Tests with Errors	Error Rate (%)	Object Count	Average Login Time (s)
			1	22.468
2	1	100	1	42.827
4	6	100	1	8.033
5	1	100	1	7.809
1	6	100	1	19.358
6	1	100	1	3.89
	1	16.67	1	16.023
4	1	100	1	22.074
			1	16.398
	4	66.67	1	24.296
	2	33.33	1	24.735
			1	32.005
1	1	100	1	7.483
			1	18.888
			1	12.962
4	1	100	1	2.222
4	1	100	1	69.088
5	1	100	1	12.95
			1	7.689
4	1	100	1	2.313
			1	19.945
			1	17.779
1	1	100	1	36.903
6	1	100	1	3.335

7. Create Time Analysis Dataset

	User Name	User ID	Password Type Code	Password Type Name	Password Name	Object Count	Create Start Time	Create End Time	Create Duration (ms)	Create Duration (seconds)
2	P01	0suGsZcE6kaN81A0tyvNI	compass_pro_viii	Compass Pro VIII	System A	6	2025-12-06 04:20:20	2025-12-06 04:22:15	115489	115.49
3	P01	0suGsZcE6kaN81A0tyvNI	compass_pro_iv	Compass Pro IV	System B	6	2025-12-06 04:15:41	2025-12-06 04:17:17	95730	95.73
4	P01	0suGsZcE6kaN81A0tyvNI	compass_lock_viii	Compass Lock VIII	System C	6	2025-12-06 04:09:22	2025-12-06 04:11:12	109773	109.77
5	P01	0suGsZcE6kaN81A0tyvNI	compass_lock_iv	Compass Lock IV	System D	6	2025-12-06 04:04:12	2025-12-06 04:05:41	88418	88.42
6	P02	1eotTEIMaeQ7ce8D71Df	compass_lock_iv	Compass Lock IV	System D	4	2025-11-15 12:22:36	2025-11-15 12:23:35	59823	59.82
7	P03	1Ih3PIHbBAbwp5fVvdWM	compass_pro_viii	Compass Pro VIII	System A	6	2025-09-03 08:11:08	2025-09-03 08:12:18	69319	69.32
8	P03	1Ih3PIHbBAbwp5fVvdWM	compass_pro_iv	Compass Pro IV	System B	4	2025-09-03 08:07:13	2025-09-03 08:07:43	30240	30.24
9	P03	1Ih3PIHbBAbwp5fVvdWM	compass_lock_viii	Compass Lock VIII	System C	6	2025-09-03 08:00:15	2025-09-03 08:01:55	99837	99.84
10	P03	1Ih3PIHbBAbwp5fVvdWM	compass_lock_iv	Compass Lock IV	System D	5	2025-09-03 07:56:47	2025-09-03 07:57:51	64642	64.64
11	P04	2Xktl6ZlYFdM5GJo3AxdL(	compass_pro_viii	Compass Pro VIII	System A	5	2025-12-01 01:51:14	2025-12-01 01:52:21	67001	67
12	P04	2Xktl6ZlYFdM5GJo3AxdL(	compass_pro_iv	Compass Pro IV	System B	5	2025-12-01 01:45:46	2025-12-01 01:47:50	124321	124.32
13	P04	2Xktl6ZlYFdM5GJo3AxdL(	compass_lock_viii	Compass Lock VIII	System C	5	2025-12-01 01:38:17	2025-12-01 01:40:26	128745	128.75
14	P04	2Xktl6ZlYFdM5GJo3AxdL(	compass_lock_iv	Compass Lock IV	System D	6	2025-12-01 01:32:00	2025-12-01 01:34:10	129158	129.16
15	P05	2pmyPlC5NnaPondS5gGC	compass_pro_viii	Compass Pro VIII	System A	4	2025-11-11 12:49:30	2025-11-11 12:50:00	30292	30.29
16	P05	2pmyPlC5NnaPondS5gGC	compass_pro_iv	Compass Pro IV	System B	4	2025-11-11 12:46:50	2025-11-11 12:47:30	40581	40.58
17	P05	2pmyPlC5NnaPondS5gGC	compass_lock_viii	Compass Lock VIII	System C	4	2025-11-11 12:42:32	2025-11-11 12:43:24	52198	52.2
18	P05	2pmyPlC5NnaPondS5gGC	compass_lock_iv	Compass Lock IV	System D	4	2025-11-11 12:39:17	2025-11-11 12:40:19	61825	61.83
19	P06	3YPFTAjel1S4ysf4kIJ4Bay	compass_pro_viii	Compass Pro VIII	System A	4	2025-12-01 04:41:15	2025-12-01 04:43:15	120128	120.13
20	P06	3YPFTAjel1S4ysf4kIJ4Bay	compass_pro_iv	Compass Pro IV	System B	4	2025-12-01 04:37:25	2025-12-01 04:38:25	60619	60.62
21	P06	3YPFTAjel1S4ysf4kIJ4Bay	compass_lock_viii	Compass Lock VIII	System C	4	2025-12-01 04:31:13	2025-12-01 04:32:36	82919	82.92
22	P06	3YPFTAjel1S4ysf4kIJ4Bay	compass_lock_iv	Compass Lock IV	System D	4	2025-12-01 04:26:10	2025-12-01 04:27:18	67613	67.61
23	P07	4e78s4cndFWN0ufQ2pPf	compass_pro_viii	Compass Pro VIII	System A	5	2025-11-12 01:53:10	2025-11-12 01:55:21	130034	130.03
24	P07	4e78s4cndFWN0ufQ2pPf	compass_pro_iv	Compass Pro IV	System B	5	2025-11-12 01:50:12	2025-11-12 01:50:55	42576	42.58
25	P07	4e78s4cndFWN0ufQ2pPf	compass_lock_viii	Compass Lock VIII	System C	5	2025-11-12 01:44:32	2025-11-12 01:45:41	68852	68.85

Create Duration (minutes)	Duration Category	Password Created At
1.92	Moderate (1-2 min)	2025-12-06 04:22:15
1.6	Moderate (1-2 min)	2025-12-06 04:17:17
1.83	Moderate (1-2 min)	2025-12-06 04:11:12
1.47	Moderate (1-2 min)	2025-12-06 04:05:41
1	Fast (30-60s)	2025-11-15 12:23:35
1.16	Moderate (1-2 min)	2025-09-03 08:12:18
0.5	Fast (30-60s)	2025-09-03 08:07:43
1.66	Moderate (1-2 min)	2025-09-03 08:01:55
1.08	Moderate (1-2 min)	2025-09-03 07:57:51
1.12	Moderate (1-2 min)	2025-12-01 01:52:21
2.07	Slow (2-5 min)	2025-12-01 01:47:50
2.15	Slow (2-5 min)	2025-12-01 01:40:26
2.15	Slow (2-5 min)	2025-12-01 01:34:10
0.5	Fast (30-60s)	2025-11-11 12:50:00
0.68	Fast (30-60s)	2025-11-11 12:47:30
0.87	Fast (30-60s)	2025-11-11 12:43:24
1.03	Moderate (1-2 min)	2025-11-11 12:40:19
2	Slow (2-5 min)	2025-12-01 04:43:15
1.01	Moderate (1-2 min)	2025-12-01 04:38:25
1.38	Moderate (1-2 min)	2025-12-01 04:32:36
1.13	Moderate (1-2 min)	2025-12-01 04:27:18
2.17	Slow (2-5 min)	2025-11-12 01:55:21
0.71	Fast (30-60s)	2025-11-12 01:50:55
1.15	Moderate (1-2 min)	2025-11-12 01:45:41

Code Sample

1. Image Wrapping Algorithm:

```
private int handleEdgeWrapping(int objRow, int objCol, int
targetRow, int targetCol) {
        // Check if target position is outside the grid
        boolean rowOutside = targetRow < 0 || targetRow >=
GRID_SIZE;
        boolean colOutside = targetCol < 0 || targetCol >=
GRID_SIZE;

        // If target is within grid, return normal position
        if (!rowOutside && !colOutside) {
            return targetRow * GRID_SIZE + targetCol;
        }

        // Handle wrapping based on which boundaries are
crossed
        int wrappedRow = targetRow;
        int wrappedCol = targetCol;

        // Handle row wrapping
        if (targetRow < 0) {
            wrappedRow = GRID_SIZE - 1; // Wrap to bottom
        } else if (targetRow >= GRID_SIZE) {
            wrappedRow = 0; // Wrap to top
        }

        // Handle column wrapping
        if (targetCol < 0) {
            wrappedCol = GRID_SIZE - 1; // Wrap to right
        } else if (targetCol >= GRID_SIZE) {
            wrappedCol = 0; // Wrap to left
        }

        return wrappedRow * GRID_SIZE + wrappedCol;
    }
```

2. Generate Test 5x5 Grid and Ramdon Compass Rotation:

```
private void generateTestGrid() {
            // Clear existing grid
            gridItems.clear();
            for (int i = 0; i < TOTAL_CELLS; i++) {
                gridItems.add(new GridItem("",
GridItem.Type.EMPTY));
            }

            // Randomly determine compass rotation
            currentCompassRotation = new Random().nextInt(4);

            // Use fixed challenge set, only shuffle positions
            List<Integer> availablePositions = new
ArrayList<>();
            for (int i = 0; i < TOTAL_CELLS; i++) {
                availablePositions.add(i);
            }
            Collections.shuffle(availablePositions);

            passwordObjectPositions = new ArrayList<>();

            // Place password objects in random positions
            List<ObjectDirectionPair> pairs =
passwordData.getObjectDirectionPairs();
            for (int i = 0; i < pairs.size(); i++) {
                ObjectDirectionPair pair = pairs.get(i);
                int position = availablePositions.get(i);
                passwordObjectPositions.add(position);

                gridItems.set(position, new
GridItem(pair.getObjectName(),
GridItem.Type.PASSWORD_OBJECT));
            }
            // Fill remaining positions with filler images
            int fillerIndex = pairs.size();
            for (int i = pairs.size(); i < TOTAL_CELLS; i++) {
                int position = availablePositions.get(i);
                String imageName =
challengeSet.get(fillerIndex % challengeSet.size());
                gridItems.set(position, new
GridItem(imageName, GridItem.Type.FILLER));
                fillerIndex++;
            }

            updateUI();
            gridAdapter.notifyDataSetChanged();
        }
```

3. Authentication Password Algorithm:

```
private void validatePassword() {
            if (!isPasswordComplete) {
                showToast("Please complete entering your
password sequence");
                return;
            }

            long loginTime = SystemClock.elapsedRealtime() -
currentTestStartTime;

            // Get user's entry password and compass direction
            String entryPassword = getEntryPassword();
            String compassNorthDirection =
getCurrentCompassDirection();

            Log.d("TestDebug", "=== Test " + currentTestNumber
+ " Results ===");
            Log.d("TestDebug", "Entry Password: " +
entryPassword);
            Log.d("TestDebug", "Compass North Direction: " +
compassNorthDirection);
            Log.d("TestDebug", "Compass Rotation Degrees: " +
(currentCompassRotation * 90));

            // Expected sequence validation
            String expectedSequenceString =
passwordData.getObjectFormat();
            List<String> expectedDirections =
extractDirectionsFromObjectFormat(expectedSequenceString);
            List<String> rotatedExpectedDirections = new
ArrayList<>();
            for (String dir : expectedDirections) {

rotatedExpectedDirections.add(rotateDirectionLabel(dir,
currentCompassRotation));
            }

            boolean isCorrect =
userDirectionSequence.equals(rotatedExpectedDirections);

            Log.d("TestDebug", "Expected Password (DB): " +
expectedSequenceString);
            Log.d("TestDebug", "Expected Directions (Rotated):
" + rotatedExpectedDirections);
            Log.d("TestDebug", "User Input Directions: " +
userDirectionSequence);
```

```
            Log.d("TestDebug", "Validation Result: " +
isCorrect);

            // Create TestResult with all required information
            TestResult result = new TestResult();
            result.setTestNumber(currentTestNumber);
            result.setSuccess(isCorrect);
            result.setLoginTime(loginTime);
            result.setTimestamp(System.currentTimeMillis());

            // NEW: Set Entry Password and Compass Direction
properly
            result.setEntryPassword(entryPassword);

result.setCompassNorthDirection(compassNorthDirection);

result.setCompassRotationDegrees(currentCompassRotation * 90);

            // Set object name (this is important for
FirebaseManager)

result.setObjectName(passwordData.getPasswordName()); // Use
password name as object name

            // Set other required fields
            result.setChallengeSet(challengeSet);

result.setTotalObjectsInSequence(passwordData.getObjectDirecti
onPairs().size());
            result.setSequenceComplete(true);
            result.setErrorCount(errorCount);
            result.setStatus(isCorrect ? "SUCCESS" :
"FAILED");

            // Set additional fields for compatibility
            result.setExpectedDirection(String.join(",",
rotatedExpectedDirections));
            result.setCompassDirection(compassNorthDirection);

            testResults.add(result);

            Log.d("TestDebug", "Test Result Created: " +
result.toString());
            Log.d("TestDebug", "Entry Password: " +
result.getEntryPassword());
            Log.d("TestDebug", "Compass Direction: " +
result.getCompassNorthDirection());
```

```
            // NEW: Save current test result to Firebase
immediately
            saveCurrentTestResult(result);

            showValidationResult(isCorrect);

            new Handler(Looper.getMainLooper()).postDelayed(()
-> {
                if (isTestInProgress) startNextTest();
            }, 2000);
        }
```

4. Direction Determination algorithm:

```
private void onGridItemClicked(int clickedPosition) {
    if (!isTestInProgress || isPasswordComplete) return;


    int totalObjects =
passwordData.getObjectDirectionPairs().size();
    if (currentObjectIndex >= totalObjects) return;

    performClickVibration();

    ObjectDirectionPair expectedPair =
passwordData.getObjectDirectionPairs().get(currentObjectIndex)
;

    int objectPosition = -1;
    for (int i = 0; i < gridItems.size(); i++) {
        GridItem it = gridItems.get(i);
        if (it.type == GridItem.Type.PASSWORD_OBJECT &&
expectedPair.getObjectName().equals(it.imageName)) {
            objectPosition = i;
            break;
        }
    }
    if (objectPosition == -1) {
        showToast("Object not found in grid.");
        return;
    }

    String userDir =
computeUserDirectionFromClick(objectPosition,
clickedPosition);

    userDirectionSequence.add(userDir);
    currentObjectIndex++;
```

```
    GridItem clicked = gridItems.get(clickedPosition);
    clicked.isSelected = true
gridAdapter.notifyItemChanged(clickedPosition);


    String expectedRaw =
expectedPair.getDirection().replaceAll("[↑→↓←↗↘↙↖]", "");
    String expectedRotated = rotateDirectionLabel(expectedRaw,
currentCompassRotation);
    if (!expectedRotated.equals(userDir)) {
        errorCount++;
    }

    if (currentObjectIndex < totalObjects) {
        updateStatus();
    } else {
        isPasswordComplete = true;
        btnLogin.setEnabled(true);

btnLogin.setBackgroundTintList(getResources().getColorStateLis
t(R.color.compass_primary, null));
        updateProgressIndicators();
        tvStatusText.setText("Click Login to validate.");

tvStatusText.setTextColor(Color.parseColor("#4CAF50"));
    }
}
```

5. Direction offset calculation algorithm:

```
private int[] getDirectionOffset(String direction) {
    switch (direction) {
        case "N":
            return new int[]{-1, 0};
        case "NE":
            return new int[]{-1, 1};
        case "E":
            return new int[]{0, 1};
        case "SE":
            return new int[]{1, 1};
        case "S":
            return new int[]{1, 0};
        case "SW":
            return new int[]{1, -1};
        case "W":
            return new int[]{0, -1};
        case "NW":
            return new int[]{-1, -1};
        case "Center":
            return new int[]{0, 0};
        default:
            return new int[]{0, 0};
    }
}
```

Poster

FINAL YEAR PROJECT II · COMPUTER SCIENCE

GRIDLOCK

Picture-Based Password Scheme to Resist Shoulder Surfing Attacks

A Compass-Based Graphical Authentication System Using Object + Direction Logic

AUTHOR: Wong Ling Cent
SUPERVISOR: Dr. Ku Chin Soon
PROGRAMME: Bachelor of Computer Science (Hons)
INSTITUTION: Universiti Tunku Abdul Rahman (UTAR)

01 INTRODUCTION

- Text-based passwords suffer from **poor memorability** and inherent security vulnerabilities.
- Existing graphical alternatives remain **highly susceptible** to shoulder-surfing attacks in real-world environments.
- **GridLock** introduces a compass-based scheme designed to decouple physical input from the actual password secret.

02 OBJECTIVES

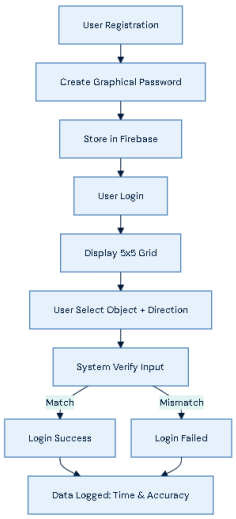
- Evaluate system **usability** — login speed and authentication success rate across sessions.
- Assess absolute **resistance** to shoulder-surfing attacks under controlled conditions.
- Analyze **long-term memorability** through a 7-day longitudinal user study.

03 SYSTEM OVERVIEW

- **Android application** integrated with Firebase Authentication & Firestore for real-time data sync.
- Operates on a **5×5 dynamic grid** using Object + Direction authentication logic.
- Automated backend logging with **millisecond-level precision** for performance analysis.

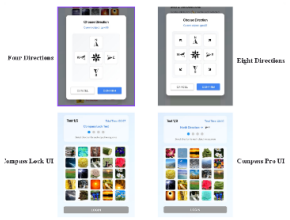
04 METHODOLOGY

- **Recognition-based** graphical password logic — users identify memorized objects and apply directional offsets.
- Experiment conducted with participants over **7 days** to evaluate usability and long-term memorability.
- Shoulder-surfing resistance validated through **controlled observation trials** across all four prototypes.



05 PROTOTYPES EVALUATED

Compass Lock IV	Compass Lock VIII
Static cardinal orientation — 4 directions	Static cardinal orientation — 8 directions
Compass Pro IV	**Compass Pro VIII**
Dynamic randomized rotation — Mental Rotation required	Dynamic randomized rotation — Mental Rotation required



06 RESULTS HIGHLIGHT

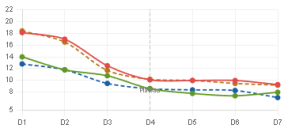
0% Breach rate across all shoulder-surfing trials

11.5s Mean login time (Compass Lock IV)

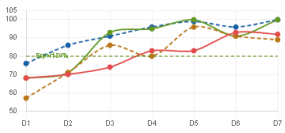
↓ 32% Login speed improvement, Day 1 → Day 7

Day 4 Cognitive plateau reached — users stabilized login speed and overcame the learning curve

MEAN LOGIN TIME OVER 7 DAYS (S)



SUCCESS RATE OVER 7 DAYS (%)



Sys A (Pro VIII) Sys B (Pro IV) Sys C (Lock VIII) Sys D (Lock IV)

07 CONCLUSION

- Dynamic compass rotation **successfully neutralizes** observation-based attacks.
- Initial cognitive complexity is quickly offset by **rapid muscle-memory adaptation**.

GridLock balances maximum security with long-term memorability — proving that a 5-object sequence is the optimal "Sweet Spot".

08 FUTURE WORK

- Enhance UI/UX and integrate **biometric multi-factor authentication (MFA)**.
- Expand testing to larger, more diverse demographic groups.

BACHELOR OF COMPUTER SCIENCE (HONS) · UTAR · FYP II · SUPERVISED BY DR. KU CHIN SOON