Word-Pattern: Enhancement of Usability and Security of User-Chosen Recognition Textual Password

Hassan Wasfi[1], Richard Stone[2], Ulrike Genschel[3]
Iowa State University, HCI Department, Iowa, USA[1]
Iowa State University, Industrial and Manufacturing, Systems Engineering Department, Iowa, USA[2]
Iowa State University, Statistics Department, Iowa, USA[3]

***Abstract*—Knowledge-based authentication systems are the most common methods used to verify users' identity, especially textual passwords. However, periodic changes in password complexity exacerbate human's limitations of remembering hard passwords over time. Therefore, a novel authentication method called Word Pattern Recognition Textual Password (WPRTP) was proposed to overcome these issues. WPRTP is based on drawing pattern on a grid with a specific security requirement to balance between usability and security. This paper aims to compare WPRTP with a recall passphrase to explore its potential for enhancing user experience, usability, and security. Fifty-four users evaluated the efficiency of WPRTP on memorability, registration time, and login time. The results indicated that WPRTP is significantly more memorable over long-term periods, with a 100% success rate, and required less registration time (29 seconds for WPRTP and 122 seconds for recall passphrase). Additionally, WPRTP users demonstrated faster login times (20 seconds for WPRTP and 42 seconds for recall passphrase). Thus, WPRTP is a potential alternative to conventional authentication methods. Future work will focus on systematically managing and reducing the tendency among users to depend on familiar, repetitive patterns in the creation of a weak password.**

***Keywords*—Authentication; password; passphrase; recognition; recall; pattern; usability; security**

I. Introduction

Authentication systems have been devised to prevent unauthorized access to sensitive data by verifying the user's identity before granting access to a system or application. Several authentication methods have been established, such as knowledge-based (e.g. username and password), biometric (fingerprint), and token-based (e.g., identification card) [1], [2]. Previous research has suggested many options to replace knowledge-based systems to enhance the security by utilizing tokens (e.g., smart cards) for authentication. However, the additional hardware required for utilizing tokens that could led to lose access to credentials if the device gets lost or stolen[3]. As another alternative, biometrics (such as fingerprints) are effective for device authentication. However, they are not easily replaceable if compromised or harmed [4]. Still, alphanumeric passwords, as one of the knowledge-based authentication systems, remain the most commonly used compared to others, particularly for online and computer applications services such as cloud services, email, and shopping [5], [6]. Nevertheless, individuals often face difficulties remembering complicated alphanumeric passwords. This causes them to either choose simple passwords or write their passwords down [7], which can cause serious security threats. These drawbacks have led to the proposition of an alternative technique called a passphrase [8], [9], [10], [11].

A passphrase is a concatenation of multiple words or phrases in a natural language, which can be easier to recall than a conventional password [12]. A study has shown that passphrases provide less cognitive effort than standard passwords, and it does not need to be changed as frequently as standard passwords [13]. In addition, longer passphrases expand the password space, enhancing their resistance against brute force attacks [14]. Unfortunately, empirical evidence has demonstrated that users commonly generate easy passphrases that include common words, typically according to patterns found in natural language [15], [16]. Moreover, a long passphrase increases typographical errors, thus causing an increase in unsuccessful login rates [17], [18]. Therefore, users usually tend to use most commonly phrase or simply reuse them with a slight change for several accounts which cause high cognitive load, potentially resulting in password fatigue and creating weak passwords vulnerable to various attacks[19].

Recognition-based textual password, that is passwords based on selecting words from predetermined list of words, are proposed to address the inherent weaknesses of recall textual password systems (traditional and passphrase password), including the cognitive effort required for memorization. This approach has been examined with two different strategies: system-assigned and user-chosen recognition-based textual passwords. The system-assigned strategy is usually more secure due to its reduced predictability and resistance to common human errors, such as selecting easy passphrase [20], [21], [22], [23]. Unfortunately, adopting this method often compromises memorability [8], requiring more training time to improve user retention [24]. On the other hand, the user-chosen passphrase is frequently based on personal selection, which may cause a security issue if a predictable passphrase is chosen [25], [26]. A physiological study comparing user-chosen and system-generated passphrases found that user-created passphrases produce fewer cognitive load stressors on working memory than system-generated passphrases [27]. Consequently, this study proved that user-chosen passphrases significantly had higher recall performance than system-assigned passphrases.

The comparison of the efficiency of different textual authentication systems (both recognition and recall) revealed that user-chosen recognition textual passwords can offer a higher memorability rate compared to recall passphrase, as they leverage human memory's strength in recognizing familiar information in long term memory [25]. Reducing the cognitive load can enhance security practices by encouraging users to create complex passwords. This approach still needs further research regarding the balance between usability and security simultaneously. WPRTP is proposed as a novel method that can stimulate human memory by combining recognition and pattern-based strategies, and this way, potentially improving retrieval performance and at the same time increasing the password space.The study primary goal is to address the challenge of password creation and recall, where users struggle to balance memorability and security, often resulting in vulnerable choices, cognitive strain, and frequent resets that compromise overall system integrity.

II. Literature Review

The literature review focuses on knowledge-based authentication systems, specifically the system-assigned and user-chosen textual password approaches. This section will discuss these two systems to provide an overview of their security implications, usability, and effectiveness of the authentication process.

A. *System Assigned Textual Password*

A study assessed the memorization of system-assigned traditional passwords and passphrases and showed that passphrases had a recall rate of 51% and passwords had a recall rate of 65% [28]. This study indicated that a comparable levels of user frustration and inconvenience, causing most users to write down their passwords. Another study examined the efficacy of textual passwords with three different categories: word recognition (passphrase), letter recall, and word recall (passphrase) with a 29-bit theoretical password space, finding no significant differences in memorability between the categories but the recognition password had significantly fewer password resets compared to word recall [20]. Another approach known as a gridWordX was proposed as hybrid knowledge-based authentication scheme combining text and graphical elements [22]. In this study, the evaluation of the usability of gridWordX (recognition nouns) compared to traditional text-based passwords revealed that gridWordX offers almost the same memorability rate compared to text-based passwords. A study established a cognitive psychology method called loci (spatial and visual memory) by utilizing video support in training sessions to enhance memorability rate but it had the drawback of a lengthy registration duration of 160 seconds [29]. Moreover, recent research improved the memorization of system-generated recognition textual passwords by applying verbal and graphical (image) cues with a high success rate but a long registration time required 265 seconds and low password space 20 bits [24]. A recent study demonstrates how using system-generated textual passwords results in lengthy training, registration, and login times [30]. As a result of that system-generated passwords possess their own set of challenges as it has a major a usability issues still, user-chosen textual passwords are more user-friendly due to their ease of use and familiarity.

B. *User-Chosen Textual Password*

User-chosen textual passwords are preferred more frequently by users compared to system-assigned passwords as they are usually easy to remember but are often predictable [31]. An approach called guided word choice increased the password space of recognition passphrase with high password entropy by selecting six words from an array of 100 or 20 words [26]. However, this approach was requiring high cognitive load as the success login rate is 46% that belong to different types of errors which are missing words order, or missing words of the phrase. A recent paper discussed user behavior and memorability of user-chosen recognition and recall textual passwords for nouns and passphrases, indicating that recognition conditions are more memorable than recall textual passwords. However, some participants in the recognition noun group forgot their passwords and requested a password reminder because they randomly generated passwords that lacked word associations in the provided word set [25]. Overall, these studies show that remembering more words from a word set can cause a cognitive burden when retrieving them in long term memory.

System-assigned and user-chosen recognition textual password research was based on storing several words, whether with a meaningful or unmeaningful association, that negatively influence memorability and security level. The main challenge of this study is establishing a new approach only partially based solely on words from a grid and psychologically enhancing the user's memorability. For this reason, WPRTP is proposed to stimulate user memory through a drawing pattern strategy, as well as enhancing the security by integrating security policies and guidelines to achieve the goal of balancing between usability and security.

III. Methodology

The study procedures followed a standardized computer configuration and participants used the same computer for all sessions within a controlled laboratory setting to eliminate any external variables that could affect experimental results, thus enhancing the overall study reliability.

A. *Participants*

This study recruited 54 participants via flyers including 31 males and 23 females ranging in age between 19 and 49 years as shows in Table I. The flyers contained detailed study information and were distributed to Iowa State University students and locals. All participants provided consent before participating in the study. The research procedures were conducted in accordance with ethical guidelines and approved by the Human Institutional Review Board (IRB), Iowa State University Compliance.

B. *Experimental Design*

The main objective of this study was to evaluate the password memorability, login time, and registration time for both recognition and recall textual passwords. A between-subject design was adopted to evaluate three independent variables: recognition noun, recognition passphrase, and recall passphrase. One-way ANOVA was performed, and all participants were distributed randomly between groups. The study

TABLE I. Demographic Information of Population

Group	Number of participants	Gender	Age Average
Recognition Noun	18	10 Males & 8 Females	29.05
Recognition Passphrase	18	11 Males & 7 Females	28.72
Recall Passphrase	18	10 Males & 8 Females	28.16

lasted for three weeks to evaluate the short and long-term memory performance. The password entropy was measured for both recognition and recall passwords using an Omni calculator [32].

The recognition groups were given a password security requirement as shown below and were advised to follow a specific guideline while creating their pattern to avoid commonly used patterns [33].

- The recognition noun and passphrase password security requirements:
  1) The word pattern should be 16 cells or more ($> 90 bits$).
  2) Use one pattern or more.
  3) Avoid predictable word pattern (predictable words association, simple shapes, predictable starting points, common patterns, use random gestures, and vary the direction and angles).
  4) Easy to remember but difficult to guess.

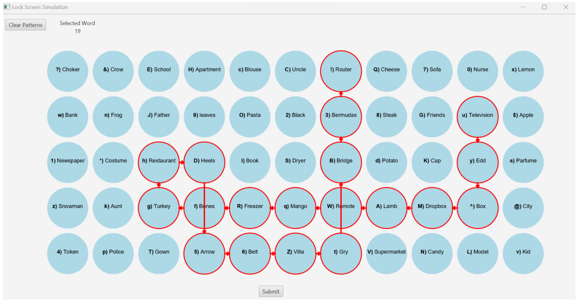
The recall passphrase group was guided by the passphrase recommended by different organizations. The passphrase users should build their password based on security requirements as shown below and follow the guideline that requires substituting letters with digits or symbols such as “Iowa w1nters are c0ld!” [34] or shortcut some words “6MonkeysRLooking^” [35].

- The recall passphrase security requirements:
  1) The passphrase should be 14 characters or more ($> 90 bits$).
  2) A combination of uppercase letters, lowercase letters, numbers, and symbols.
  3) Do not use common words or personal information.
  4) Easy to remember but hard to guess. Consider utilizing a memorable passphrase.

C. Apparatus

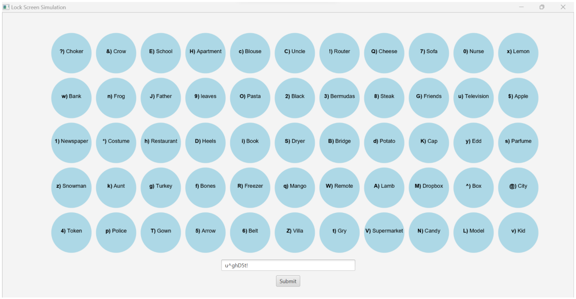
The recognition noun and passphrase password were based on randomly generating 55 words from a predefined word pool. Each generated word is assigned a random alphanumeric character or special symbols. The main goal of using characters is that the users must enter the corners of their created pattern to successfully log in. For example, the characters of the drawn pattern in Fig. 1 “uy^MAwqRfghD56ZtB3!” are stored in the database but the user is required in the login phase to enter the corners of the pattern as “u^ghD5t!” as shown in Fig. 2 and the system will automatically gather the characters in between to compare it to the saved password in the database. The user can create more than one pattern and the system demonstrates these patterns with different colors: the first pattern is red, the second is blue, and the third is green. Furthermore, each pattern is accompanied by a starting arrow to highlight the point of origin and the endpoint of the pattern. In the login phase, when users build more than one pattern, they should separate between the characters of each pattern with space to successfully login. For instance, the characters of the drawn patterns in Fig. 3 are “n^QLqVOvbozuJUPs” and “C#y” are stored in the database, but the user is required in the login phase to enter the corners of patterns separated with space as “n^bouJs C#y” as shown in Fig. 4 and the system will automatically gather the characters in between for both patterns and compare it to the saved password in the database. The random word generation system consists of the following components:

1) Word pool A pool with a variety of common word types including nouns, adjectives, and verbs (881 words) to ensure their applicability for native speakers and foreigners. The concrete nouns were chosen because they are more memorable than abstract nouns [36].
2) Character set A set of alphanumeric characters and special symbols to randomly assign a character to each word generated from the word pool: “ABCDEFGHIJKLMNOPQRSTUVWXY Zabcdefghijklm nopqrstuvwxyz0123456789!@#$%^&*()-_+=[]{}:;’¡¿,.?/—‘̃”.



?) Choker	&) Crow	E) School	H) Apartment	c) Blouse	C) Uncle	!) Router	Q) Cheese	7) Sofa	0) Nurse	x) Lemon
w) Bank	n) Frog	J) Father	9) leaves	O) Pasta	2) Black	3) Bermudas	8) Steak	G) Friends	u) Television	$) Apple
1) Newspaper	*) Costume	h) Restaurant	D) Heels	i) Book	S) Dryer	B) Bridge	d) Potato	K) Cap	y) Edd	s) Parfume
z) Snowman	k) Aunt	g) Turkey	f) Bones	R) Freezer	q) Mango	W) Remote	A) Lamb	M) Dropbox	^) Box	@) City
4) Token	p) Police	T) Gown	5) Arrow	6) Belt	Z) Villa	t) Gry	V) Supermarket	N) Candy	L) Model	v) Kid

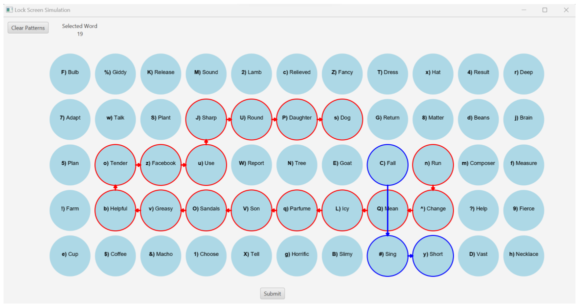
Fig. 1. The registration interface for the recognition noun pattern.



?) Choker	&) Crow	E) School	H) Apartment	c) Blouse	C) Uncle	!) Router	Q) Cheese	7) Sofa	0) Nurse	x) Lemon
w) Bank	n) Frog	J) Father	9) leaves	O) Pasta	2) Black	3) Bermudas	8) Steak	G) Friends	u) Television	$) Apple
1) Newspaper	*) Costume	h) Restaurant	D) Heels	i) Book	S) Dryer	B) Bridge	d) Potato	K) Cap	y) Edd	s) Parfume
z) Snowman	k) Aunt	g) Turkey	f) Bones	R) Freezer	q) Mango	W) Remote	A) Lamb	M) Dropbox	^) Box	@) City
4) Token	p) Police	T) Gown	5) Arrow	6) Belt	Z) Villa	t) Gry	V) Supermarket	N) Candy	L) Model	v) Kid

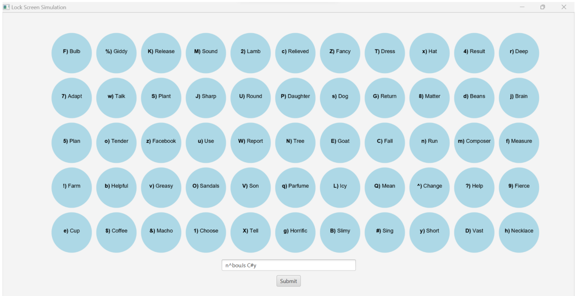
u^ghD5t!

Fig. 2. The login interface for the recognition noun pattern.



Selected Word
19

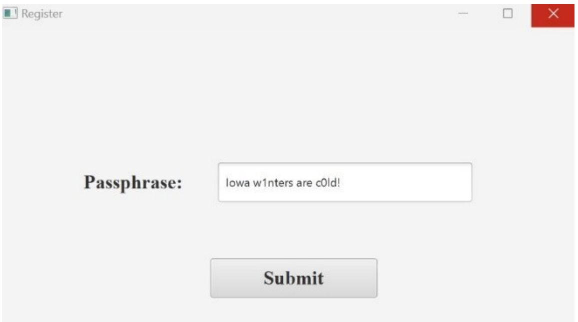
Fig. 3. The registration interface for the recognition passphrase pattern.



n^bouJs C#y

Fig. 4. The login interface for the recognition passphrase pattern.

In contrast, for the recall passphrase, an interface was created to allow participants to enter a passphrase considering particular security rules as shown in Fig. 5.



Passphrase: Iowa w1nters are c0ld!

Fig. 5. The registration and login interface for the recall passphrase.

D. Procedure

Detailed information about the research objectives and study procedures was presented to participants to ensure clarity and understanding and eliminate any potential bias before commencing the study. The study lasted three weeks to determine factors that can influence the success rate and login time for short- and long-term memory.

- **Session 1:** The first session comprises a series of distinct steps:
  - **Password Creation:** The participants were instructed to generate a password following the given password security requirements.
  - **Short-term memory (STM):** After password creation, the participants were distracted for a few seconds and then asked to log in to evaluate the short-term memory. If a participant incorrectly entered their password three times, they were provided with a password reminder.
  - **Answer Pre-survey:** The participants answered demographic questions.
- **Session 2 (Long-Term Memory 1 (LTM1)):** One week after Session 1, the participants were required to return to assess their long-term memorability of their passwords and login time performance. If participants incorrectly entered their password three times, they were given a reminder.
- **Session 3 (Long-Term Memory 2 (LTM2)):** Two weeks after Session 2, the participants were required to return to evaluate long term memorability of their passwords and login time performance. If participants incorrectly entered their password three times, they were given a reminder. They were then asked for feedback to assess the user experience of their assigned password approach.

IV. Result

All data were analyzed using SPSS 28. We used a One-way ANOVA to assess mean differences in registration time, login time and memorability depending on treatment (authentication condition) followed by Tukey's HSD for post-hoc comparisons to test hypotheses 1 – 9. A check of the ANOVA assumptions revealed lack of Normality for all dependent variables and differences in the variances between treatment groups, leading us to repeat the analyses using the non-parametric Kruskal Wallis Test. Because the results were qualitatively the same, we present the ANOVA results that we suspect most readers are more familiar with. In the literature, robustness of ANOVA against violations of Normality and unequal variances has been repeatedly established, especially when sample sizes are equal across treatment groups as is the case in our study [37], [38].

A. Registration Time

H1. There will be a significant difference in the mean registration time between user-chosen recognition nouns compared to recall passphrases.

H2. There will be a significant difference in the mean registration time between user-chosen recognition passphrases compared to recall passphrases.

H3. There will be a significant difference in the mean registration time between user-chosen recognition nouns compared to recognition passphrases.

Before testing hypotheses H1 through H3, a one-way ANOVA test was conducted to ensure that at least one of the three group means was different based on the global F-test (F = 19.027, df = 2, 51, $p < .001$). The post-hoc pairwise comparisons indicated the following differences in the mean registration times between password types: the recognition noun approach was statistically highly significant different (mean difference = 83 seconds, $p < .001$) compared to the recall passphrase, indicating longer registration times for the recall passphrase. Likewise, the recognition passphrase approach was statistically highly significant (mean difference = 93 seconds, $p < .001$) compared to the recall passphrase group, also indicating longer registration times for the recall passphrase as shown in Fig. 6. However, there was no significant difference between recognition noun and recognition passphrase (mean difference= 10 seconds, p = .819).

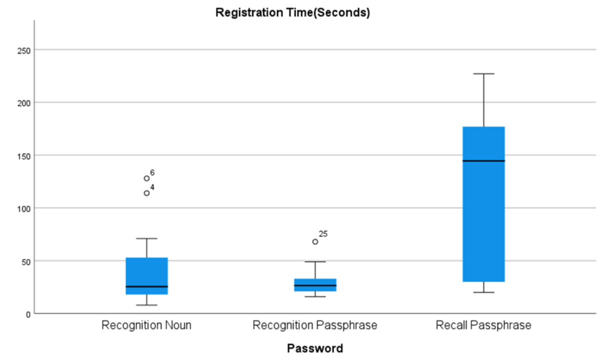


Fig. 6. The registration performance in seconds for each authentication condition. The black horizontal line in the boxplots denotes the median registration time for all participants in the treatment group.

B. Login Time

H4. There will be a significant difference in mean login time between user-chosen recognition nouns compared to recall passphrases in STM and LTM.

H5. There will be a significant difference in mean login time between user-chosen recognition passphrases compared to recall passphrases in STM and LTM.

H6. There will be a significant difference in mean login time between user-chosen recognition nouns compared to recognition passphrases in STM and LTM.

A one-way ANOVA test was conducted to examine the difference in mean login time between the three types of passwords across three memory conditions: STM, LTM1, and LTM2. The results revealed that no significant difference exists between all groups in STM (F = 1.896, df=2, 51, p = .161). Similarly, there was no significant difference between them in login time in LTM1 (F = .694, df=2, 51, p = .504), but there was a significant difference in LTM2 (F = 3.564, df = 2, 51, p =.036), indicating that the type of password interaction significantly impacts login times in this memory condition. The post hoc Tukey HSD test indicated no significant difference in login time for STM and LTM1 conditions but in LTM2, recognition nouns significantly took less time to login compared to recall passphrase (mean difference = 22 seconds, p = .036) as shown in Fig. 7. Overall, the login time results of the three-period showed same pattern of login time in STM and LTM2 however, in LTM1, both recognition groups presented an increase in login time and a decrease in the recall passphrase group. However, In the LTM2, the login time for both recognition passwords is reduced and increased for recall passphrase, which indicating that recognition passwords with practice become more efficient, while the recall passphrase group needed more time to login due to increased cognitive demand.

C. Memorability

H7. There will be a significant difference in the memorability rate between user-chosen recognition nouns compared to recall passphrases in STM and LTM.

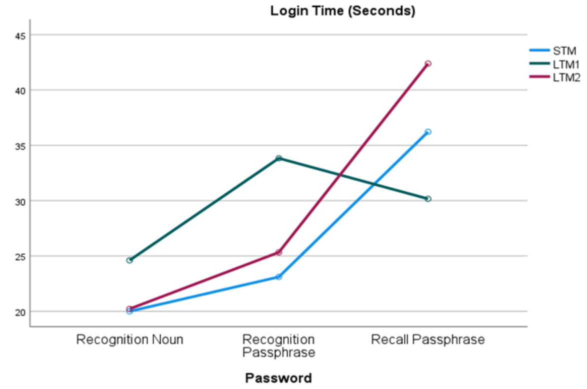


Fig. 7. The login time average per authentication condition.

H8. There will be a significant difference in the memorability rate between user-chosen recognition passphrases compared to recall passphrases in STM and LTM.

H9. There will be a significant difference in the memorability rate between user-chosen recognition nouns compared to recognition passphrases in STM and LTM.

A one-way ANOVA test was conducted to examine the difference in mean memorability rate from the first attempt between the three types of passwords across three memory conditions: STM, LTM1, and LTM2. In the analysis of memorability rate from the first attempt among different password types, the ANOVA results revealed significant differences between groups in STM based on the global F-test (F (2, 51) = 5.921, p = .005). Post hoc comparisons using the Tukey HSD test indicated significant mean differences between several groups. Specifically, recognition noun had a significantly higher mean memorability rate compared to recall passphrase (mean difference = 0.27778, p = .027). Similarly, recognition passphrase also significantly had higher memorability rate compared to recall passphrase (mean difference = 0.33333, p = .006). Conversely, the differences between recognition noun and recognition passphrase were not statistically significant (p = .854).

The LTM1 results revealed no significant difference in memorability rate based on global F-test (F (2,51) = 2.410 and p=.100). The post hoc comparisons using the Tukey HSD test examined the mean differences, though they did not reach statistical significance between all groups. The closest to significance was the difference between recognition noun and recall passphrase (mean = 0.27778 and p = .084), suggesting a trend where recognition noun might lead to better memorability than recall passphrase. However, the LTM2 memorability results showed a highly significant difference in memorability rate between groups (F (2, 51) = 10.818, $p < .001$). Post hoc comparisons using the Tukey HSD revealed significant differences where both recognition noun and recognition passphrase is significantly outperformed recall passphrase in memorability rate (mean difference = 0.38889 and $p < .001$). However, no significant difference was found between recognition noun and recognition passphrase, indicating that both types of recognition-based passwords performed higher in terms of long-term memorability as compared to the recall passphrase, as shown in Fig. 8.

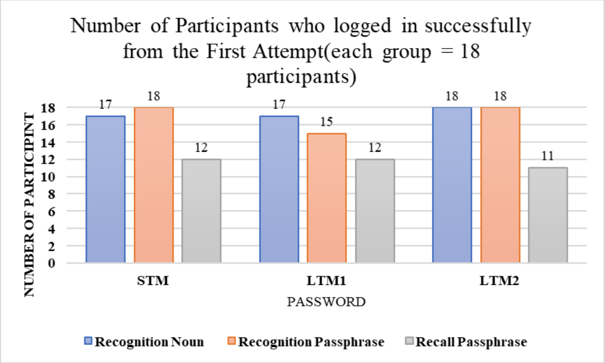


Fig. 8. The successfully login rate from the first Attempt per authentication conditions.

These results offer a detailed insight into the effects of recognition patterns (nouns and passphrases) compared to recall passphrases on registration speed, login efficiency, and memory retention. Thus, the three-week study proved that recognition pattern passwords significantly outperform in memorability and login time compared to recall passphrases. Th user experience was also evaluated using a 10-point Likert scale showing that the users preferred the WPRTP methods (noun and passphrase) in terms of ease of creation, memorability, entry speed with practice, preference over text-based passwords, and perceived security as shows in Table II. Pattern-based techniques performed better in areas such as memory and simplicity of creation, showing how effective they are in improving the user experience and reducing cognitive burden. These results highlight WPRTPs as a potential alternative to recall passphrases as they offer a balance between security and usability.

TABLE II. The Main Questions and Scores for Pattern Nouns, Pattern Passphrase and Recall Passphrase Participants

Question/Score(average)	Noun Pattern	Passphrase Pattern	Passphrase Recall
Is it easy to create?	8.27	8.5	6.27
Is it easy to remember?	9.29	8.88	6.16
With practice, I could quickly enter password?	9.52	9.83	8.33
Do you Prefer it compared to text-based password?	8.11	7.83	7
Do you think it is secure?	9.23	9.66	8.66

Discussion

This section will discuss the results of the WPRTP and recall passphrase over a three-week study to distinguish its efficiency and user satisfaction of both methods in term of login time, memorability, and how these factors can impact on authentication as shown in Table III. The study findings proved that WPRTP had a superior memorability rate compared to recall passphrase for long term period. Both recognition nouns and passphrase pattern showed 100% successed rate from the first attempt in LTM2 however, no improvement in succeed rate of recall passphrase which presented 61.11% on the first attempt and slightly increased to 72.22% in the third attempts in LTM2. During the three weeks, 22.22% of recall passphrase participants requested a password reminder with no enhancement in memorability rate thus, displaying difficulty in retrieving the correct password, which caused an increase in the login time from 30 in LTM1 to 42 seconds in LTM2. On the other hand, both recognition passwords login time is decreased from 24 to 20 seconds for recognition noun and 33 to 25 seconds for recognition passphrase. Therefore, these differences between WPRTP and recall passphrase underscores the cognitive load and challenges inherent in recall-based method. There were several usability challenges and limitations that influence participants performance for all groups but increasingly for recall passphrase. The WPRTP participants found difficulty during entering the corners of their patterns but with practice they were more adopted and efficiently executing their pattern accurately. The login errors were occurred because of:

- 60% of the participants had errors called missing corner error (occurred when participants forgot one corner or more of their pattern).
- 40% of the participants had a case letter error (occurred when participants used capital letter instead of small letters or vice versa of their attached characters of patterns).

On the other hand, recall passphrase participants had a major issue of retrieving phrase that include numbers, symbols, and mixed-case letters with substitution strategy. Notably, the participants who had more than one symbol or substitutes characters in the phrase or both together result in confusion in retrieving the correct password. Also, long passphrase with specific requirements raises the possibility of spelling error. Despite of users acquired password reminders but still no improvement in memorability in long term memory. There are several errors that influence significantly the memorization such as:

- 54.54% of the participants had a special character/digit error (occurred when participants forgot special character and/or digit or insert more special character and/or digit in the phrase). Example, password is (May!StandUnshkn03*) and the error was forgetting the symbol * in the end of the phrase(May!StandUnshkn03).
- 36.36% of the participants had a spelling error (occurred when the participants written word incorrectly). Example, password is (Ames1scold@thisyear).
- 9.1% of the participants had substitute errors (occurred when participants forgot the exact substituted character position). Example, the password created is (Ultra high performance concrete 1s str0ng!) and the error was forgetting changing the letter “i” in “is” with 1 (Ultra high performance concrete is str0ng!).

User behavior is essential in creating memorable and secure word pattern passwords. Using password policies and guidelines helped to mitigate user’s behavior, such as selecting easy or predictable word patterns. From the drawn patterns, it found that implementing the minimum requirement of a 16-

TABLE III. THE SUCCESSFUL LOGIN RATE, REGISTRATION TIME AND LOGIN TIME FOR RECOGNITION NOUN AND PASSPHRASE AND RECALL PASSPHRASE

The Success rate for Recognition and Recall textual password					
Noun Pattern					
	1st attempt	2nd attempt	3rd attempt	Registration Time (Average in seconds)	Login time (Average in seconds)
STM	94.44%	100%	100%	39	20
LTM1	94.44%	100%	100%		24
LTM2	100%	100%	100%		20
Passphrase Pattern					
	1st attempt	2nd attempt	3rd attempt	Registration Time (Average in seconds)	Login time (Average in seconds)
STM	100%	100%	100%	29	23
LTM1	83.33%	100%	100%		33
LTM2	100%	100%	100%		25
Passphrase Recall					
	1st attempt	2nd attempt	3rd attempt	Registration Time (Average in seconds)	Login time (Average in seconds)
STM	66.66%	77.77%	77.77%	122	36
LTM1	66.66%	83.33%	83.33%		30
LTM2	61.11%	66.66%	72.22%		42

word pattern decreases the tendency to connect words with a semantic meaning or another relationship. For instance, some participants tried to select words based on association, but when they connected them with a pattern, they failed to meet the minimum pattern length of 16 words. This requirement forced them to select patterns with no logical links between words. For instance, Fig. 1 showed that participant was trying to connect Television with Turkey which has the same first letter but it was not met the required length thus, led to increase the pattern to Router word. Also, most participants built their pattern by avoiding predictable word associations, simple shapes, predictable starting points, and common patterns. These rules motivate them to create patterns with changes and multiple overlaps, thus demonstrating complexity in their pattern approach. For example, Fig. 3 presented two patterns with unstructured linguistics passphrase: first pattern was based on two parts (run helpful and use dog) and the second pattern was based on the position of the beginning of the first pattern. However, there are some recognized weak behaviors, such as using patterns with less vary in directions relying on memorization without engaging securely robust and random patterns. Therefore, these findings presented the importance of thoughtfully designed password policies and guidelines, but still some tools needed to ensure the security level of word pattern password as discussed in the future work below.

V. CONCLUSION AND FUTURE WORK

This study demonstrated WPRTP's advantages in terms of memorability and ease of use compared to recall passphrases. Significantly, WPRTP offered a more memorable solution, potentially reducing the risk of password resets, as constantly forgetting, and resetting passwords causes user fatigue [39]. There are some limitations recognized in the study include the following; small sample size of the participants. Moreover, the experiment was conducted in a laboratory setting, which means the results not reflects the actual real-life performance. Future study should be performed on large samples with increased gender, age, and ethnic diversity to support and expand the WPRTP approach. Also, future research should enhance pattern security using algorithms that reduce the predictability of patterns within the word grid as follows:

- Pattern analysis and predictability modeling: use machine learning methods to evaluate the predictability of the created pattern.
- Randomization algorithm: use an algorithm to encourage or enforce the creation of less predictable patterns.

REFERENCES

[1] D. Palma and P. Luca Montessoro, "Biometric-Based Human Recognition Systems: An Overview," Recent Advances in Biometrics, pp. 1–21, 2022, doi: 10.5772/intechopen.101686.

[2] H. Wasfi and R. Stone, "Usability and Security of Knowledge-based Authentication Systems: A State-of-the-Art Review," 2023. [Online]. Available: www.ijacsa.thesai.org

[3] F. Schwarz, K. Do, G. Heide, L. Hanzlik, and C. Rossow, "FeIDo: Recoverable FIDO2 Tokens Using Electronic IDs: Solving Token Loss and User Data Privacy via TEE-protected Attribute-based Credentials," in Proceedings of the ACM Conference on Computer and Communications Security, Association for Computing Machinery, Nov. 2022, pp. 2581–2594. doi: 10.1145/3548606.3560584.

[4] A. Roy, N. Memon, and A. Ross, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems," IEEE Transactions on Information Forensics and Security, vol. 12, no. 9, pp. 2013–2025, Sep. 2017, doi: 10.1109/TIFS.2017.2691658.

[5] T. H. E. Landscape, O. F. Authentication, C. Survey, E. Younis, and S. J. Mohammed, "Saja J. MOHAMMED 2," pp. 1–16, 2023.

[6] H. Adamu, A. D. Mohammed, S. A. Adepoju, and A. O. Aderiike, "A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication," Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022, pp. 1–5, 2022, doi: 10.1109/NIGERCON54645.2022.9803122.

[7] Y. S. Chuen, M. Al-Rashdan, and Q. Al-Maatouk, "Graphical password strategy," Journal of Critical Reviews, vol. 7, no. 3, pp. 102–104, 2020, doi: 10.31838/jcr.07.03.19.

[8] N. Jagadeesh and M. V. Martin, "Alice in Passphraseland: Assessing the Memorability of Familiar Vocabularies for System-Assigned Passphrases," arXiv [cs.CR], 2021.

[9] A. Addas, J. Thorpe, and A. Salehi-Abari, "Geographic Hints for Passphrase Authentication," 2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings, 2019, doi: 10.1109/PST47121.2019.8949033.

[10] G. Nielsen, M. Vedel, and C. D. Jensen, "Improving usability of passphrase authentication," 2014 12th Annual Conference on Privacy, Security and Trust, PST 2014, pp. 189–198, 2014, doi: 10.1109/PST.2014.6890939.

[11] A. Mukherjee, K. Murali, S. K. Jha, N. Ganguly, R. Chatterjee, and M. Mondal, MASCARA: Systematically Generating Memorable And Secure Passphrases, vol. 1, no. 1. Association for Computing Machinery, 2023. [Online]. Available: http://arxiv.org/abs/2303.09150

[12] J. Madrid, Y. Levy, L. Dringus, and L. Wang, "Towards the Development and Assessment of a Method for Educating Users into Choosing Complex, Memorable Passphrases," 2022, doi: 10.32727/28.2023.4.

[13] B. Bhana and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," Computers & Security, vol. 96, p. 101925, Sep. 2020, doi: https://doi.org/10.1016/j.cose.2020.101925.

[14] K. Juang, "Integrating Visual Mnemonics and Input Feedback with Passphrases to Improve the Usability and Security of Digital Authentication Recommended Citation," 2014. [Online]. Available: https://tigerprints.clemson.edu/all_dissertations

[15] P. B. Maoneke, S. Flowerday, and M. Warkentin, "Evaluating the usability of a multilingual passphrase policy," 26th Americas Conference on Information Systems, AMCIS 2020, pp. 0–10, 2020.

[16] C. Bonk, Z. Parish, J. Thorpe, and A. Salehi-Abari, "Long Passphrases: Potentials and Limits," 2021 18th International Conference on Privacy, Security and Trust, PST 2021, pp. 1–7, 2021, doi: 10.1109/PST52912.2021.9647800.

[17] S. Sahin and F. Li, "Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication," Proceedings of the ACM Conference on Computer and Communications Security, pp. 252–270, 2021, doi: 10.1145/3460120.3484791.

[18] B. Mohinder Singh and N. Jaisankar, "Efficient and Secure Sound-Based Hybrid Authentication Factor with High Usability," KSII Transactions on Internet and Information Systems, vol. 17, no. 10, pp. 2844–2861, 2023, doi: 10.3837/tiis.2023.10.014.

[19] A. Nosenko, Y. Cheng, and H. Chen, "Password and Passphrase Guessing with Recurrent Neural Networks," Information Systems Frontiers, vol. 25, no. 2, pp. 549–565, Apr. 2023, doi: 10.1007/s10796-022-10325-x.

[20] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password? Applying recognition to textual passwords," SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security, 2012, doi: 10.1145/2335356.2335367.

[21] H. Assal, A. Imran, and S. Chiasson, "An exploration of graphical password authentication for children," Int J Child Comput Interact, vol. 18, pp. 37–46, 2018, doi: 10.1016/j.ijcci.2018.06.003.

[22] U. Cil and K. Bicakci, "gridwordx: Design, implementation, and usability evaluation of an authentication scheme supporting both desktops and mobile devices," Workshop on Mobile Security Technologies (MoST13), 2013.

[23] Z. Joudaki, J. Thorpe, and M. V. Martin, "Reinforcing system-assigned passphrases through implicit learning," Proceedings of the ACM Conference on Computer and Communications Security, pp. 1533–1548, 2018, doi: 10.1145/3243734.3243764.

[24] M. N. Al-Ameen, S. T. Marne, K. Fatema, M. Wright, and S. Scielzo, "On improving the memorability of system-assigned recognition-based passwords," Behaviour and Information Technology, vol. 41, no. 5, pp. 1115–1131, 2022, doi: 10.1080/0144929X.2020.1858161.

[25] H. Wasfi and R. Stone, "The Effectiveness of Applying Different Strategies on Recognition and Recall Textual Password," International Journal of Network Security & Its Applications, vol. 14, no. 2, pp. 15–29, 2022, doi: 10.5121/ijnsa.2022.14202.

[26] N. K. Blanchard, C. Malaingre, and T. Selker, "Improving security and usability of passphrases with guided word choice," pp. 723–732, 2018, doi: 10.1145/3274694.3274734.

[27] L. A. Loos, Minas. K, R. Crosby., and M. E. M.-B C. Ogawa, Passphrase authentication and individual physiological differences, vol. 12776 LNAI. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-78114-9_19.

[28] R. Shay et al., "Correct horse battery staple: Exploring the usability of system-assigned passphrases," SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security, 2012, doi: 10.1145/2335356.2335366.

[29] S. M. T. Haque, M. N. Al-Ameen, M. Wright, and S. Scielzo, "Learning System-assigned Passwords (up to 56 Bits) in a Single Registration Session with the Methods of Cognitive Psychology," Proceedings of the Network and Distributed System Security Symposium (NDSS 2017), vol. 17, 2017, doi:10.14722/usec.2017.23034.

[30] F. N. Meem et al., "A Practical Scheme to Improve Memorability of System-assigned Random Password," Dhaka University Journal of Applied Science and Engineering, vol. 7, no. 1, pp. 29–37, Feb. 2023, doi: 10.3329/dujase.v7i1.62884.

[31] T. Tanni, T. Taharat, M. Parvez, S. Rumee, and M. Zaber, "Is My Password Strong Enough?: A Study on User Perception in The Developing World," EAI Endorsed Transactions on Creative Technologies, vol. 9, no. 30, p. 173452, Mar. 2022, doi: 10.4108/eai.11-2-2022.173452.

[32] A. Szczepanek, "Password Entropy Calculator." Accessed: Apr. 21, 2024. [Online]. Available: https://www.omnicalculator.com/other/password-entropy.

[33] P. Andriotis, G. Oikonomou, and T. Tryfonas, "A Study on Usability and Security Features of the Android Pattern Lock Screen Author Details," 2016.

[34] Iowa University, "What is the difference between a password and a passphrase? — Information Technology Services," its.uiowa.edu. https://its.uiowa.edu/support/article/2549

[35] Microsoft, "Create and use strong passwords," 2022. Accessed: Sep. 07, 2022. [Online]. Available: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

[36] L. J. Hamilton and E. S. Allard, "Words matter: age-related positivity in episodic memory for abstract but not concrete words," Aging, Neuropsychology, and Cognition, vol. 27, no. 4, pp. 595–616, Jul. 2020, doi: 10.1080/13825585.2019.1657556.

[37] E. Schmider, M. Ziegler, E. Danay, L. Beyer, and M. Bühner, "Is It Really Robust?: Reinvestigating the robustness of ANOVA against violations of the normal distribution assumption," Methodology, vol. 6, no. 4, pp. 147–151, 2010, doi: 10.1027/1614-2241/a000016.

[38] M. J. Blanca, R. Alarcón, J. Arnau, R. Bono, and R. Bendayan, "Effect of variance ratio on ANOVA robustness: Might 1.5 be the limit?," Behavior Research Methods, vol. 50, no. 3, pp. 937–962, Jun. 2017, doi: https://doi.org/10.3758/s13428-017-0918-2.

[39] A. S. George, "The Dawn of Passkeys: Evaluating a Passwordless Future," 2024, doi: 10.5281/zenodo.10697886.