Enhanced Textual Password Scheme for Better Security and Memorability

Hina Bhanbhro
Department of Computer Syst. Eng.
Faculty of Electrical, Electronics & Computer Systems Engineering
Shaheed Benazir Bhutto University

Syed Raheel Hassan
Department of Computer Science
Faculty of Computing and Information Technology
King Abdulaziz University

Shah Zaman Nizamani
Department of I.T.
Faculty of Science
Quaid-e-Awam University

Sheikh Tahir Bakhsh, Madini O.Alassafi
Department of Information Technology
Faculty of Computing and Information Technology
King Abdulaziz University

***Abstract*—Traditional textual password scheme provides a large number of password combinations but users generally use a small portion of available password space. Complex textual passwords are difficult to remember, therefore most users choose passwords with small length and contain dictionary words. Due to the use of small password length and dictionary words, textual passwords become easy to crack through offline guessability attacks. Traditional textual passwords scheme is also weak against keystroke logger attacks because alphanumeric characters are directly inserted into the password field. In this paper, enhancements are proposed in the registration and login screen of the traditional textual password scheme for improving security against offline guessability attacks and keystroke logger attacks. The proposed registration screen also improve memorability of traditional textual passwords through visual cues or pattern-based approach. In the proposed login screen, passwords are indirectly inserted into the password field, to resist keystroke logger attacks. A comparative analysis between the passwords created in traditional and proposed pattern-based approach is presented. The testing results show that users create strong and high entropy passwords in the proposed pattern-based approach as compared to the traditional textual passwords approach.**

***Keywords*—Security; usability; alphanumeric passwords; authentication**

I. Introduction

When users have the freedom to select any textual password, they select weak passwords or they select predictable password patterns [1]. Weak passwords can be guessed through dictionary attacks or brute force attacks [2]. The processing power of computing machines is increasing over time [3], due to which offline guessability attacks such dictionary and brute-force attacks become less effort taking. To resist offline guessability attacks, the users are encouraged to create strong textual passwords by using different password setting policies.

Password-based authentication techniques are called knowledge-based authentication techniques. In these techniques, passwords can be graphical or textual. Graphical passwords consist of some graphical elements such as pictures or drawings. Textual passwords consist of some combinations of alphanumeric characters. Graphical passwords contain visual cues for password memorization, therefore they are considered better than textual passwords in terms of password memorability. However, the graphical passwords are weak against shoulder surfing attacks because they can be easily viewed. Complex textual passwords are difficult to memorize, therefore users use dictionary words in their textual passwords. This approach makes textual passwords vulnerable to dictionary attacks.

A. Password Memorization Techniques

In the category of knowledge-based authentication, textual passwords are most widely used for authentication. However, users set easy to guess or weak textual passwords due to memorability limitations [2]. The textual passwords which contain mix of alphanumeric characters, and have high length are better for security but such passwords are difficult to memorize. Different techniques are suggested by researchers for memorizing hard to guess (strong) passwords, the techniques are listed here:

(a) Passphrase
(b) Cognitive passwords
(c) Associative passwords
(d) Mnemonic passwords

a) Passphrase: Passphrase is a set of words that together form a password. Passphrases are generally easy to remember and difficult to guess because they contain large number of alphanumeric characters. For example, the passphrase "clean the table at the corner" contains 29 characters and it is also easy to memorize due to logical meaning of the phrase.

b) Cognitive passwords: In cognitive passwords, a series of questions are asked and the users are authenticated when correct answers are given. The users select the set of questions and their answers. For example, "What is the name of your birth place?" Cognitive passwords are difficult to guess because the attackers have to correctly identify both questions and answers. These passwords are weak in terms of useability because selecting questions and writing answers take some time.

c) Associative passwords: In associative passwords, the users select some dictionary words provided by the system and their related textual response. For example, "wall=painting". These passwords are difficult to guess because it is difficult to identify the words used as passwords. Associative passwords are easy to memorize for one or two user accounts but it becomes difficult when large number of associative passwords are required to be remembered.

d) Mnemonic passwords: In this technique of password memorization, a complete sentence is memorized by a user and the password consists of the first letter of each word of the sentence. For example, the sentence "Birth date of Aliza is on 1st May" can be memorized for the mnemonic password "BdoAio1M". Through this approach random alphanumeric characters of a password can be easily remembered.

All the above password memorization techniques help in memorization of strong passwords but recalling multiple passwords for different accounts is a difficult task in all the password memorization techniques. Users feel difficulty in correctly recognizing which password belongs to which user account. These password memorization techniques also require some mental effort for recalling the passwords [4], therefore the techniques are not widely used by the users.

In this paper, some enhancements are suggested in password registration and login screens of the traditional textual password scheme for better memorization of passwords. In the proposed enhancements, visual cues can be added to the random alphanumeric characters of the password by using the pattern-based approach. The visual cues help in memorization of strong alphanumeric passwords and through the proposed pattern-based approach, the users'behavior of setting weak passwords can also be changed.

The remaining paper is divided into five sections. In Section 2 literature review is given about the problems in traditional textual passwords. Research methodology for pattern-based passwords is explained in Section 3. In Section 4 analysis of pattern-based approach is presented. Finally the conclusion is given in Section 5.

II. Related Work

Textual passwords were first analyzed by Morris and Thompson in 1979 [5]. They found that 86% of the passwords were weak e.g. passwords had small length, consisting of lowercase letters only, digits only or mixture of the two with dictionary words. After Morris and Thompson [5] a large number of studies have been done on understanding the characteristics of textual passwords set by the users. Researchers from Microsoft carried out a study [6] that involved half a million web-based passwords. From the study, the researchers found that users generally create weak passwords and they reuse the same password across multiple accounts. Same password weaknesses were also found by Smith [7] and Borges *et al.* [8]. These studies suggest that a large number of textual passwords can be cracked through dictionary attacks. klein [9] performed a dictionary attack on 15,000 passwords through the password dictionary of 3000000 alphanumeric strings. Klein [9] successfully cracked 25% passwords through the dictionary attack. The research studies on textual passwords highlight the need for motivating users for setting strong or secure passwords.

Liu *et al.* [10] analyzed the length of textual passwords set by the users, the researchers found that majority of users set passwords with a length of less than twelve alphanumeric characters. The result of Liu *et al.* [10] shows that small portion of textual password space is being used by the users, as a result different offline guessability attacks become easy to apply [11].

Viktor Taneski *et al.* [12] conducted a systematic literature review of articles and journals about password use and password security. The researchers [12] suggested different password setting policies and password checkers to guide users for setting strong passwords. Password meters [13] are used in some websites for informing users about the strength of the passwords. Egelman *et al.* [14] analyzed the effect of password meters. They found that password meters do not have a significant effect on changing behavior of users, towards setting strong passwords due to memorability issues. Strict password creation policies have a poor effect on memorability [15].

Strong textual passwords contain strings of alphanumeric characters which do not belong to dictionary words and they have larger lengths [16]. Different password setting policies are applied in applications for enforcing users to set strong passwords, such as minimum length and a mix of multiple categories of alphanumeric characters. However, research studies [17] suggest that users create weak passwords even after applying password setting policies.

Due to human limitations of information memorization, users reuse the same password across different accounts. Florencio and Herley [6] found that, on average users can easily remember 6.3 different textual passwords. However, users generally have more than six accounts, therefore they reuse same password in different accounts.

The advantage of strong textual passwords decreases when the same password is re-used in multiple user accounts [18]. The attacker after cracking a password from the less secure application, apply the cracked password on more secure applications [19]. Therefore, it is also important that users should create separate passwords for different accounts. Password managers are used to create strong and distinct password for each user account. However, password managers have some security and usability issues [20] i.e. a password manager can be hacked and it may not be available all the time. Privacy is also an issue with the password managers because all the passwords will be presented into a third party software.

Cognitive or visual cues are helpful for memorization of information. Therefore, in the proposed enhancements of traditional textual password scheme, the users can draw a visual pattern from the alphanumeric characters of a password on the registration screen. The password pattern serves as visual cue for better memorization of the textual password. Pattern-based passwords help users to easily set and remember strong or secure alphanumeric passwords.

III. Research Methodology

To analyze the effect of pattern-based passwords, a user study was conducted. The user study was divided into four

phases. In the first phase, password setting trends in traditional textual passwords were analyzed through a pre-test survey. In the second phase, users were asked to register and login inside the specially designed application for testing usability, security, and memorability aspects of the pattern-based passwords. In the third phase, a post-test survey was conducted for understanding the feelings of the users about the pattern-based approach. In the fourth phase, the data of pre-test survey and application testing was analyzed for security, usability, and memorability aspects of the pattern-based approach.

For this research 110 users participated, out of which 43 were female and 67 were male. All the users belonged to different professions including students, teachers and administration staff. The users belonged to different institutions including the Quaid-e-Awam University of Engineering, Science & Technology, SZABIST Nawabshah and Shah Abdul Latif University.

A. Pre-test survey

The objective of the pre-test survey was to find out the password setting trends in traditional textual passwords. Due to privacy issues exact textual passwords were not collected from the users but they were asked to provide some information about the passwords. In the pre-test survey users were asked to provide information regarding size and type of alphanumeric characters used in their passwords. Results of the pre-test survey are shown in Table I.

TABLE I. PASSWORD TRENDS IN TRADITIONAL TEXTUAL PASSWORDS

Average password length	9.56
Lower-case letters used	87%
Upper-case letters used	19%
Numbers used	54%
Special characters used	21%

Table I shows that majority of users use lower-case letters in their passwords along with decimal numbers. Generally in computer applications, users are restricted to select at least two categories of alphanumeric characters. Decimal numbers are easy to remember along with some dictionary words. Therefore, comparably high percentage of decimal numbers are used in comparison with capital letters and special characters.

B. Application Testing

For analyzing usability and memorability aspects of pattern-based passwords, a web-based application was developed. In the application, users were asked to perform registration and login activities. Timings of registration and login activities were recorded through the testing application. Failed and successful login attempts were also saved in the database of the application.

1) Registration Activity: In the registration activity, the participants created their accounts in the testing application. Registration screen of the testing application is shown in Fig. 1. The alphanumeric characters are present on the registration screen along with profile and authentication fields as shown in Fig. 1. Different categories of alphanumeric characters are separately presented on the registration screen. For example, lower-case letters are present at the top of the screen while numbers are present at the bottom of the registration screen. This arrangement helps in recalling password characters from the password patterns.

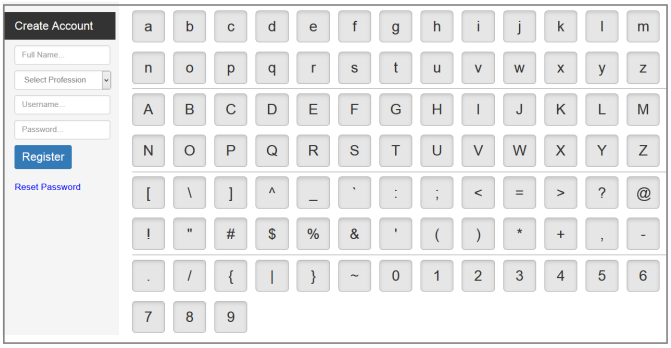

Fig. 1. Registration screen.

a) Password selection: Passwords can be entered through keyboard or mouse on the registration. Through keyboard, the passwords can be entered by pressing alphanumeric keys similar to the traditional textual password scheme. For mouse-based password entry, a user needs to drag or click over alphanumeric characters present on the registration screen. For example, if a user drags the mouse from "h" to "1", "j" to "3" and "U" to "W" then some lines will be drawn over the alphanumeric characters as shown in Fig. 2. Visually the password will look like "H" but in the database, the password *huHU;(1jwJW=*3UVW* will be saved.

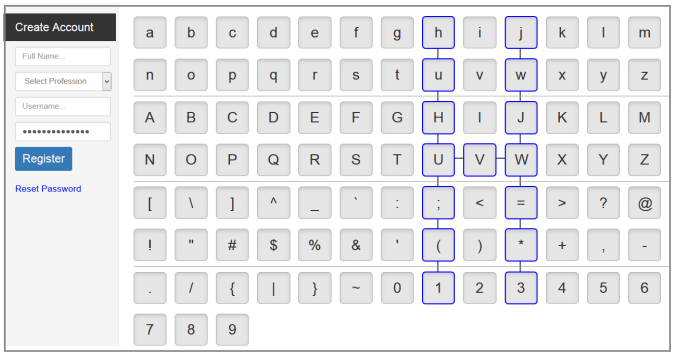

Fig. 2. Registration screen after password selection.

When the mouse is dragged multiple times over same alphanumeric characters then same password pattern will be created but alphanumeric characters will be repeated in the password. For example if a user drags the mouse two times from "h" to "1" then visually a straight line will be formed from "h" to "1" but in the database, the password *huHU;(1huHU;(1* will be saved.

Through pattern-based approach a strong textual password such as given in the example can be easily memorized by the visual cues. A user just needs to remember the visual shape of the password along with starting and ending alphanumeric characters of the password pattern.

2) Login activity: In this activity, users provide login credentials (username & password) for authentication. The login screen of the testing application is shown in Fig. 3. The login screen contains two sequences of alphanumeric

characters, one for actual password characters and other for temporary representation of the password characters. Actual alphanumeric characters (present in the button shape) are sequentially present, while representing alphanumeric characters are randomly present in the login screen i.e. they change their position in every login session. For randomization of the representing characters, Algorithm-1 can be used.

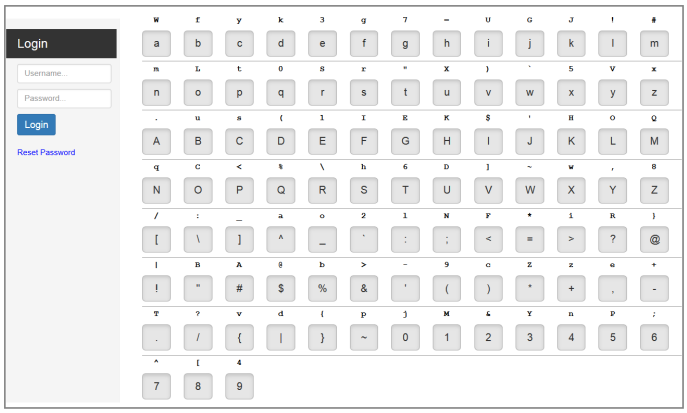

Fig. 3. Login screen.

Algorithm 1 Algorithm for Alphanumeric Characters Randomization

1: $TempElements \leftarrow list\ of\ alphanumeric\ characters$
2: $RepresentingElements \leftarrow NULL$
3: $ELength \leftarrow 95$
4: **for** $i = 0$ to 94 **do**
5: $temp \leftarrow NULL$
6: $ind \leftarrow random$(0,ELength)
7: $RepresentingElements$[i] $\leftarrow TempElements[ind]$
8: $TempElements$[i] $\leftarrow remove$(ind,$TempElements$)
9: $ELength$ $\leftarrow$ELength - 1
10: **end for**

a) Password selection: On the login screen, a password can be entered through keyboard or mouse. Passwords are entered through the keyboard by typing characters representing the password of a user. For example, if the password of a user is *huHU;(1jwJW=*3UVW* and characters representation are same is shown in Fig. 4, then the user has to type *iUrE!)PVT6Jx}>J1E* characters in the password field for authentication. In this case, first password character "h" is represented by "i" and the password character "u" is represented by "U" and so on. This temporary representation of password characters helps in avoiding keystroke logger attacks.

Mouse-based password entry requires dragging or clicking the mouse over the password characters, similar to the registration screen. For example, in the current scenario when password of a user is *huHU;(1jwJW=*3UVW* then the password can be entered by dragging mouse from "h" to "1", "j" to "3" and "U" to "W". When passwords are entered through mouse then the passwords can be observed through shoulder surfing attacks. Therefore in public, it is better to enter passwords through keyboard. For improving security against shoulder surfing attacks in case of mouse-based password entry, the process of generating password lines should be removed from the login screen. In the login screen, a link is given for reset password. This option clears all the lines drawn from the login screen and the text written in the password field.

C. Post-test Survey

After completing registration and login activities, a post-test survey was conducted. In the post-test survey five questions were asked from the users about the proposed pattern-based approach. The questions and their answers are shown in Table II. The post-test survey was conducted for understanding how comfortable users are in using the proposed pattern-based approach. The results of the post-test survey are shown in Section IV-D.

IV. Results and Discussion

After completing pre-test, post-test surveys and application testing, the data was analyzed to know the performance of pattern-based approach. From the data, security, usability and memorability aspects of pattern-based passwords were analyzed.

A. Strength of passwords

Fig. 5 shows a different types of alphanumeric characters (lower-case, upper-case letters, numbers and special characters) used in traditional and pattern-based passwords. The data for traditional textual passwords were collected from pre-test survey and the data for pattern-based passwords were collected from the database of the testing application.

Fig. 5 shows that in pattern-based passwords, upper case letters and special characters are widely used by the users as comparison with traditional textual passwords. A high percentage of capital letters and special characters in pattern-based passwords show that the dictionary attacks will be difficult to apply in the passwords of pattern-based approach.

Password length and entropy of both the password setting approaches are given in Table III. Results show that password length is slightly higher in traditional textual passwords. However, password entropy of pattern-based passwords is higher than traditional textual passwords. The password entropy shows that users create strong passwords through pattern-based approach.

B. Timings

Password entry time for pattern-based passwords were analyzed through the log stored in the database of the testing application. Average password entry time when passwords were entered through keyboard was 18.24 seconds and when passwords were entered through mouse was 7.19 seconds. The reason for higher login time in keyboard based password entries is that, users have to identify alphanumeric characters which represent the password characters from the login screen.

C. Password Memorability

To test memorability of pattern-based passwords, users were asked to perform login activities in the testing application. Memorability tests were conducted in three different timings, which were immediately after registration, after one day and

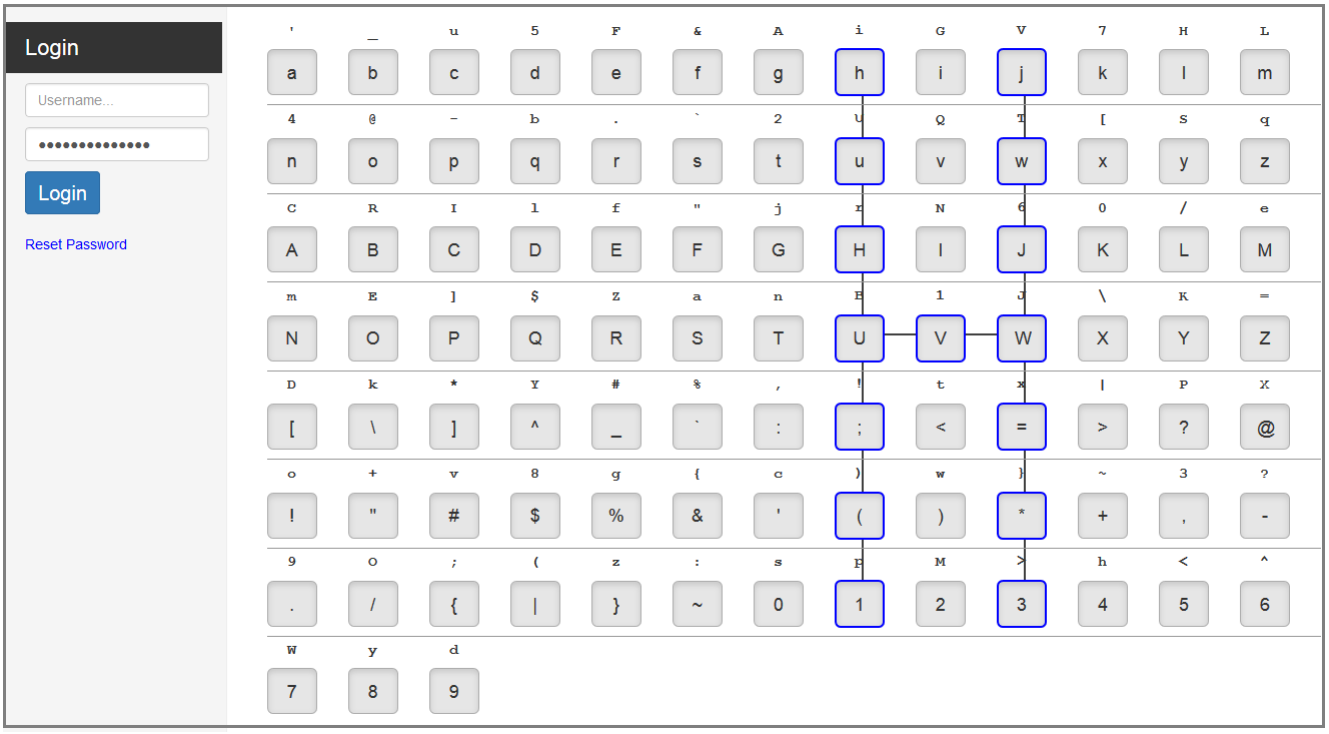

Fig. 4. Login screen after password selection.

TABLE II. POST-TEST QUESTIONNAIRE

No.	Question	Options
1	Do you think the pattern-based approach helps in password memorization?	(a) Yes (b) No (c) Little-bit
2	The pattern-based approach is most useful for?	(a) Registration page (b) Login page (c) Both of them (d) None
3	Pattern-based approach is suitable for?	(a) Desktop applications (b) Web-based applications (c) Mobile applications (d) All of them
4	How do you remember the password?	(a) Password patterns only (b) Alphanumeric characters (c) Both of them
5	How easy it is to use the pattern-based approach?	(a) Very Easy (b) Easy (c) Average (d) Difficult

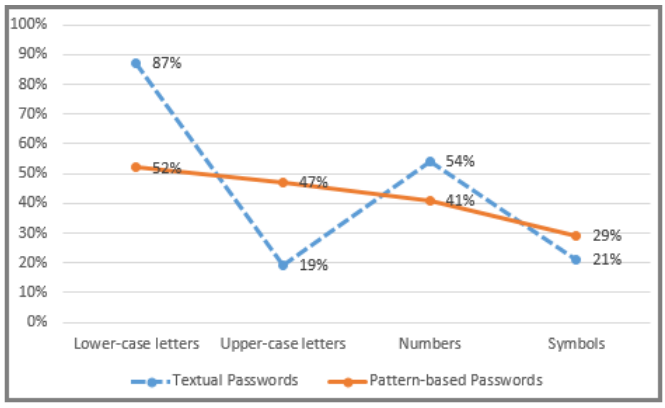

Fig. 5. Alphanumeric characters comparison.

TABLE III. PASSWORDS STRENGTH

Scheme	Password length	Password entropy
Textual passwords	9.56	53.88
Pattern-based passwords	9.21	57.62

after one week. Users were allowed maximum three attempts for a successful login.

Table IV shows password recall rate in the pattern-based approach. Results show that memorability of textual passwords is improved by the pattern-based approach. The results also show that with the passage of time password memorability decreases. In this experiment, users only interacted with the login page in specified timings (immediately after registration, after one day and one week), they were not allowed to login on 2nd to 6th day of registration. If the users were allowed to login inside the system on each day, then the memorability results would have been much better after one week duration because recalling information on short periods have positive effect on memorability.

TABLE IV. PASSWORDS MEMORABILITY

Time	1st attempt	Within 2 attempts	Within 3 attempts
Immediately after registration	83%	89%	98%
After 1 day	78%	82%	89%
After 1 week	69%	73%	76%

D. Qualitative Analysis

In the post-test survey, users were asked to share their views about the pattern-based password setting approach. In the survey five questions were asked from the users, the results are shown in Tables V to IX.

Pattern-based approach provides multiple ways (cognitive and visual) of password memorization. Therefore, users find this approach helpful for password memorization.

TABLE V. RESULTS OF QUESTION 1

Q.01: Do you think pattern-based approach helps in password memorization	
Option	**Answer**
Yes	81%
No	7%
Little-bit	12%

TABLE VI. RESULTS OF QUESTION 2

Q.02: Pattern-based approach is useful for	
Option	**Answer**
Registration page	17%
Login page	14%
Both of them	63%
None	6%

The results of Table VI show that majority of users found the proposed approach useful for both registration and login pages. The reason for this choice is that registration page helps in password memorization and login page improves password security.

TABLE VII. RESULTS OF QUESTION 3

Q.03: Pattern-based approach is suitable for	
Option	**Answer**
Desktop applications	11%
Web-based applications	68%
Mobile applications	5%
All of them	16%

Table VII shows that majority of users preferred web-based applications for the pattern-based. The web-based applications are more vulnerable to security attacks than desktop and mobile applications. The pattern-based approach improves password security, therefore this approach is most suitable for the web-based applications.

TABLE VIII. RESULTS OF QUESTION 4

Q.04: How do you remember the password	
Option	**Answer**
Password pattern only	73%
Alphanumeric characters	19%
Both of them	8%

Table VIII shows that majority of users remembered password patterns instead of alphanumeric characters of the passwords. Visual password shapes are easy to remember than random alphanumeric characters, therefore most of the users only remembered the password patterns.

Android unlock scheme is widely used by the users and the proposed pattern-based approach has similarities with the scheme. Therefore, users found easy to use the proposed pattern-based approach as shown in Table IX.

The qualitative analysis done through the post-test survey shows that users are satisfied with the performance of pattern-based approach i.e. they found pattern-based approach easy to use and helpful for password memorization. However, the majority of users prefer to use this approach in web based applications because chances of password hack are high in web based applications.

V. DISCUSSION

Many knowledge based authentication schemes are proposed which provide better security than textual password scheme. However, passwords of the secure knowledge based authentication schemes are difficult to memorize and password entry procedures are very complex. Due to memorability and usability issues, such schemes are not accepted by the software industry. Through the proposed scheme, security and memorability improvements are made in the traditional textual password scheme.

TABLE IX. RESULTS OF QUESTION 5

Q.05: How easy it is to use the pattern-based approach	
Option	**Answer**
Very easy	22%
Easy	59%
Average	14%
Difficult	5%

Although proposed scheme improves security of textual passwords against different security attacks such as dictionary attacks and keystroke logger attacks, but the proposed scheme is vulnerable to screen-scrapper attack. In this attack a password is captured by recording both password input and login screen. In the proposed scheme, one-to-one relationship exists between actual password characters and their representing alphanumeric characters for a particular session. Therefore, passwords can be captured by recording both representing password characters and screen-shot of the login screen. For further improving security of textual passwords, the proposed scheme needs to be enhanced to resist the screen-scrapper attacks.

VI. CONCLUSION

Strong textual passwords which contain mix of alphanumeric characters are difficult to memorize because they do not contain cognitive or visual cues for password memorization. Through the proposed pattern-based password setting approach, strong textual passwords become easy to memorize due to visual cues. Qualitative and quantitative results show that memorability of strong alphanumeric or textual passwords is improved through the pattern-based approach.

Users create strong textual passwords through the pattern-based approach, therefore brute-force and dictionary attacks will be difficult to apply when the pattern-based approach is used in the registration screen. Keystroke logger attacks are resisted in the proposed login screen by indirectly collecting password characters from the users.

ACKNOWLEDGMENT

The authors acknowledge the faculty members, students and administration staff of Quaid-e-Awam University, SZABIST nawabshah and Shah Abdul Latif University for helping us in performing different surveys and application testing for the research work.

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[2] A. Forget, S. Chiasson, and R. Biddle, "Helping users create better passwords: Is this the right approach?" in *Proceedings of the 3rd Symposium on Usable Privacy and Security*. ACM, 2007, pp. 151–152.

[3] G. E. Moore, "Cramming more components onto integrated circuits, electronics magazine," 1965.

[4] N. Ekstrom, "Password practice: The effect of training on password practice," 2015.

[5] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[6] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 657–666.

[7] S. W. Smith, "Humans in the loop: Human-computer interaction and security," *IEEE Security & privacy*, vol. 99, no. 3, pp. 75–79, 2003.

[8] M. A. Borges, M. A. Stepnowsky, and L. H. Holt, "Recall and recognition of words and pictures by adults and children," *Bulletin of the Psychonomic Society*, vol. 9, no. 2, pp. 113–114, 1977.

[9] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.

[10] Z. Liu, Y. Hong, and D. Pi, "A large-scale study of web password habits of chinese network users." *JSW*, vol. 9, no. 2, pp. 293–297, 2014.

[11] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: persuasive cued click-points," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*. British Computer Society, 2008, pp. 121–130.

[12] V. Taneski, M. Hericko, and B. Brumen, "Password securityno change in 35 years?" in *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on*. IEEE, 2014, pp. 1360–1365.

[13] M. Bishop and D. V. Klein, "Improving system security via proactive password checking," *Computers & Security*, vol. 14, no. 3, pp. 233–249, 1995.

[14] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?: the impact of password meters on password selection," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 2379–2388.

[15] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 2.

[16] P. C. Dean, J. Buck, and P. Dean, "Identity theft: A situation of worry," *Journal of Academic and Business Ethics*, vol. 9, p. 1, 2014.

[17] D. Florencio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?" *HotSec*, vol. 7, no. 6, 2007.

[18] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[19] B. Prince, "Twitter details phishing attacks behind password reset. eweek," 2010.

[20] Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: Security analysis of web-based password managers." in *USENIX Security Symposium*, 2014, pp. 465–479.