Usability and Security of Knowledge-based Authentication Systems: A State-of-the-Art Review

Hassan Wasfi
Iowa State University HCI Department
Iowa, USA

Richard Stone
Iowa State University Industrial and
Manufacturing Systems Engineering Department,
Iowa, USA

***Abstract*—Knowledge-based passwords are still the most dominant authentication method for securing digital platforms and services, in spite of the emergence of alternative systems such as token-based and biometric systems. This method has remained the most popular one mostly because of its usability, compatibility, affordability of implementation, and user familiarity. However, the main challenge of knowledge-based password schemes lies in creating passwords that provide a balance between memorability and security. This research aimed to compare various knowledge-based schemes in order to establish a strategy that provided high memorability and resilience to most cyberattacks. The overview of this research identifies areas of knowledge-based passwords for further research and enhances the methodology that helps to offer insight into usable, secure, and sustainable authentication approaches. Future work has been recommended to explore the major features and drawbacks of recognition-based textual passwords because this method provides the usability and security benefits of graphical passwords with the familiarity of textual passwords.**

***Keywords*—Knowledge-based authentication; recognition; recall; usability; security; memorability**

I. Introduction

The biggest challenge for several companies is to establish an authentication technique that offers a high level of usability and security. Authentication systems can be classified into three main types: knowledge-based, token-based, and biometric [1], [2]. Large corporations and banks have recently switched to the use of biometrics or token passwords to verify individuals' identities, but these passwords require expensive hardware and high-complexity algorithms [3]–[5]. However, the most usable password is the knowledge-based one, particularly the textual passwords, because it is easy to use and user-friendly and has an extendable security feature [6]. Different researchers have extensively investigated the most common password schemes, as shown in Fig. 1, including usability, security, and deployability benefits. Thus, none of the stated methods converge to the benefits of textual passwords [7], [8]. The text password security requirements have increased dramatically in the last ten years because most people are not aware of the fundamentals of creating a strong password[9]. Users tend to create weak passwords with personal information and predictable patterns, which could be easily guessed by the password owner's close people or attackers [10]. Another scheme called a passphrase has been proposed as an alternative to text-based passwords; it offers better memorability and security [11], [12]. Though, the typing of long passphrases has shown an increase in typographical errors, thus reducing the successful login rate [13]–[15]. Researchers have suggested algorithms that help avoid small typographical errors but still do not fully mitigate this issue (correct up to 57.7%) [16]. A recent study also found that 8.8% of users' passwords are vulnerable to attacks because of the typo-tolerance software [17]. There is another method considered a competitive strategy to recall passphrases called recognition-based textual passwords. The most usability-centered advantage of this scheme is to reduce the cognitive load and enhance the retrieval performance [18], [19]. Different studies have stated that a recognition passphrase has a better memorability rate than a recall scheme [19], [20]. The main usability and security challenges for recognition-based textual passwords are system design, user login performance, and resistance against guessing, brute-force, and shoulder-surfing attacks [21]. Nowadays, the knowledge-based password scheme needs further research to help to produce a system with large security entropy, low cognitive load, low cost, and resistance to common attacks. The main contribution of this paper is to analyze and evaluate the features and drawbacks of knowledge-based password schemes. We have aimed to present detailed information about the existing knowledge-based methods adopted thus far to critically investigate possible issues and, thus, help to propose ways to establish a new secure and usable knowledge-based authentication approach. This paper argues that the existing authentication systems must thoroughly address users' cognitive limitations or leverage humans', particularly for the recognition of textual passwords. Consequently, despite considerable research, establishing the recognition of textual passwords suggests a low cognition load, high memorability, and resistance to the most common attacks.

II. Related Work

This part will compare the main types of knowledge-based authentication systems, namely textual and graphical passwords.

A. Textual Passwords

1) Text-Based Passwords: The traditional text-based password has been the most common authentication method for the past two decades [22]. It has several usability characteristics, such as ease of use and low cost to establish [23]. The password's strength depends on its complexity, length, and unpredictability against a guessing attack [24]. However, people tend to use insecure strategies for password creation, such as the use of common phrases, personal information, or predictable patterns [25]. These behaviors enforce businesses to set strict password policies [26]. Unfortunately, prior research has found

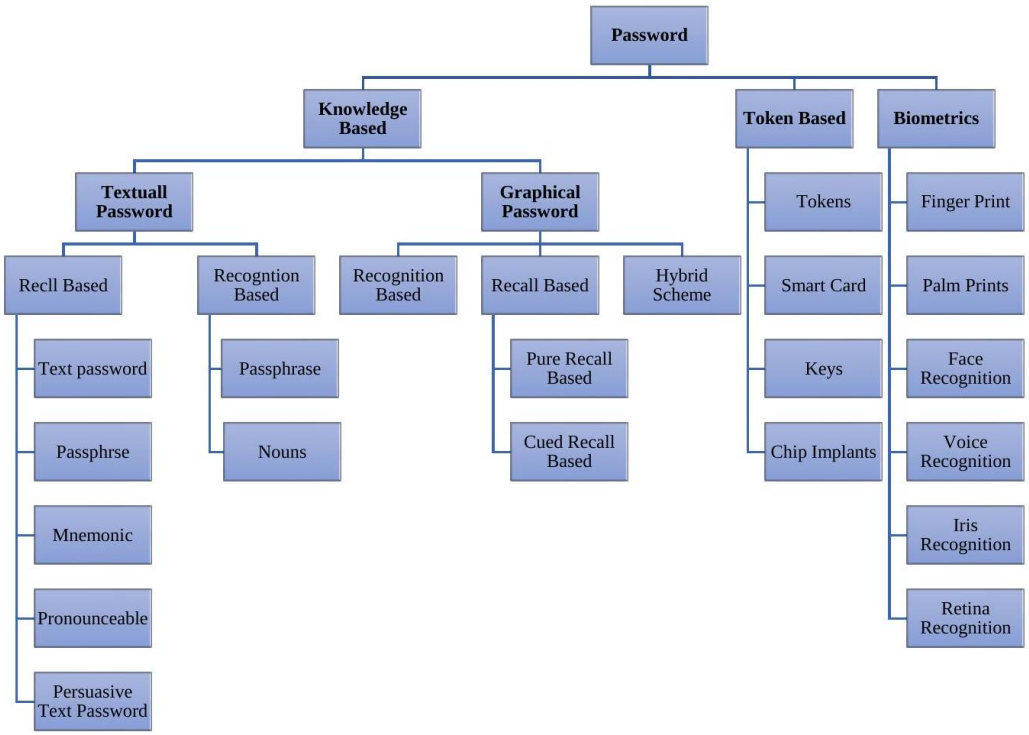

Fig. 1. Taxonomy of authentication systems.

that password policies are not sufficiently effective to form a strong password [10]. Additionally, a majority of people reuse the same passwords for different accounts because of cognitive challenges; thus, this practice might be risky as if one account is compromised, the attacker could use the same password to access the other accounts [27]. A survey result reported that 94% of the participants reused at least one password for more than one account [28].

2) Passphrases: A passphrase is a type of password that contains a series of words or text to authenticate an individual identity [29]. Long passphrases provide better security against brute-force attacks and frequently require less cognitive load than traditional passwords [30]. It was found that users spent less time on password activities such as retries and resets when using passphrases than when using traditional passwords [13]. However, a passphrase result in a usability issue related to typographical errors [13], [14], [31]. The typographical errors significantly increased when the passphrase was very lengthy [13], [19], [25] or when the guidelines and policies were followed strictly [8], [32]. In addition, people tend to create passphrases from common words with predictable patterns; this method is vulnerable to guessing attacks [33]. Regarding the previous usability and security issues of the passphrase approach, several studies have suggested the following:

- Tolerate spelling errors by applying a validation algorithm that accepts small typing errors without any influence on security entropy [34]. Still, these algorithms have a significant security degradation, not as previously understood [17].
- Create a long passphrase with specific security policies [12], [14].
- Systemically generate random words to reduce the predictability level [20], [31]. Table I lists the differences between users and system-generated passphrases.

3) Mnemonic Passwords: A mnemonic is a concept of sentence abbreviation that assists or is intended to assist memory by utilizing patterns of letters (often, the first letter), numbers, or relevant associations [35]. An analysis of mnemonics and passphrases created based on entire words shows that mnemonics offer a superior memorability rate [36]. Different mnemonic strategies are often utilized, such as sentence substitution "**IwentHK4&hya**" or special character insertion "**He,llo&&world!**" [37], [38]. Moreover, simulating the letters on keyboard buttons with different patterns to produce a mnemonic, such as "**H**" is equal to "**UHBijnhj**" [39]. Consequently, it provides a slight resistance against brute-force attacks as compared to traditional passwords [37].

4) Pronounceable Passwords: In 1975, it was established to systemically produce complex and memorable pronounceable passwords [40], [41]. The old version of the pronounceable password algorithm was vulnerable to guessing attacks if an attacker could analyze the pattern of the generated password [40]. Although systemically generated pronounceable passwords are intended to be easier to remember than random sequences of letters, but they still need further strategies. To address this issue, a study[42] suggested a method that partially combines two words while considering the phonotactic and syllabic restrictions of verbal English, which plays a role in determining the memorability rate. A new approach called "ProSemPass" is based on user-chosen pronounceable and semantically meaningful passwords; thus, it has 30% higher memorability than the systemically generated pronounceable

TABLE I. USABILITY AND SECURITY OF RECALL PASSPHRASE

Recall Passphrase			
	Memorability	**Security**	**Comment/Limitation**
User Generated	High	Low/Medium	• Needs guidelines and policies for security enhancement [14], [32] • Is easier to remember than text passwords [13] • Is easy to guess [43], [44]
System Generated	Low	High	• Is difficult to remember because of the unmeaningful passphrase structure [45]. • Is most likely to be written down[46] • Has guaranteed robustness against guessing attacks [30]

methods and is more resilient against guessing attacks [41]. Recently, a new study suggested converting a user-chosen password into phonemes and measuring their pronounceability to enhance the password's usability and security and compared this method with different pronounceable strategies, including the "ProSemPass" scheme; however, on the basis of the findings, the author recommended the use of a passphrase instead of the proposed approach because it promises better usability and security standards [47].

5) Persuasive Text Passwords (PTP): PTP is a user-chosen text password system with a random guideline to create a secure password. It is based on selecting one word, whose security will be enhanced by the system by placing a few randomly selected characters at randomly assigned positions [48]. For instance, users can select the word "security", and the PTP system will generate random changes, such as inserting or replacing the characters as "use>curity". Users can shuffle for repositioning characters until they are persuaded with a memorable password. However, the PTP does not deliver a high security level, particular after insertion, because PTP does not assess the password's strength [49].

6) Recognition-based Textual Passwords (Human Memory and Words Memorability): The human capacity to memorize large amounts of information is limited. Psychological researchers have discussed how the human brain works and how to exploit its features to transfer data from the short- to the long-term memory [50]. In 1956, Miller argued the range of items that individuals can hold for the short-term memory is approximately seven [51]. Different strategies explain how human memory pays attention to information through a human's five senses (sight, hearing, taste, smell, and touch) and is transferred from the sensory register to the short-term memory. Moreover, with rehearsal the information will be transferred to the long-term memory [52]. The capacity of the human brain to store words for a long period differs from person to person, but the stimulus to the human memory has a critical role in how information is effectively stored and retrieved [53]. In general, the major factors in the English language that have a direct impact on the memorability rate are as follows:

- Word Frequency: Several research studies have examined the memorability of high-frequency (HF) or common words versus low-frequency (LF) or uncommon words and found that the HF-word versus the LF-word memorability is complex and depends on many aspects, such as recall versus recognition, word familiarity, task nature, mixed lists, pure lists and subsequent memory [54].
- Concreteness and imageability: Concrete words are words that "refer to tangible objects, materials, or persons and can be easily perceived with the senses" and thus, stimulate the mental image [55].
- Valence: This belongs to emotional words, which are divided into two main categories: attractiveness/"good"-ness (positive valence) or averseness/"bad"-ness (negative valence) of an object, circumstance, or event [56].
- Arousal: Arousal is related to the personal experience of feelings (emotion words), including tension and high energy [57].

Word memorability in education is complex because various physiological factors play a role, such as individual memory capacity, culture, and age [58]. In authentication systems, the English words are established with different strategies as compared to the learning criteria as follows:

1) Recall or recognition strategy
2) Word-generated methodology: user-generated, system-generated, or both
3) Grid design (word presentation)
4) Word type
5) Word structure (phrase, semantic meaning, etc.)

Previous researchers have attempted to implement a recognition mechanism for different types of passwords to enhance their retrieval performance. A majority of the authentication systems based on recognition methods used graphical passwords to leverage human memory through visual information (images) [59], as discussed in Section 2.2. In contrast, the recognition approach has been used with English words but has still not yet been fully investigated. Word recognition passwords are a relatively challenging area of authentication systems because they are a less common form of authentication. They typically require the users to select specific words as passwords, which can be easier to memorize than complex text-based passwords. In the last decade, several studies have examined the recognition of words with different types of passwords, as shown in Table II.

7) User-Chosen vs. System-Assigned Passwords: User-chosen passwords are vulnerable to various attacks because users tend to create easy passwords to remember with predictable patterns [64]. Most websites force their users to create passwords conforming to specific policies; however, these policies are not sufficiently effective to generate secure passwords [65]. Extant research has proven that users have a misconception about creating strong passwords for various reasons, such as using common keyboard patterns, words, phrases, or personal information [66]. To partially

TABLE II. USABILITY AND SECURITY OF RECOGNITION OF TEXTUAL PASSWORDS

Recognition-Based Textual Passwords				
Source	**Condition**	**Memorability**	**Security**	**Comments/Limitations**
Study [20]	system-generated (a) recall password (b) recall passphrase (c) recognition passphrase	- recognition passphrase > recall passphrase, letter, password - letter recall > passphrase recall	4 words out of 156 (29.14 bits)	• Some participants commented that their passphrase did not include a verb or semantic meaning ("throat" and "tongue"), which negatively affected the retrieval of the correct password. • Recognition method has significantly fewer password resets than word recall. • Takes a long time to log in because the GUI contains six groups of words.
Study [18]	system-generated recognition (a) objects (b) image (c) words	- objects > image and words - words = image	5 words out of 48 (27.9 bits)	• No balance exists between word types presented to users in the registration phase (adjectives less than other types). • Word set contains words with the same first letters, which might confuse users in long-term memory such as "Camp" and "Lamp". • Memorizing time for words is less than that for objects and significantly less than that for images.
Study [60]	system-generated (a) recognition nouns (b) text-based password	- text-based password > recognition nouns	3 words out of 104 (20.1 bits)	• Noun recognition has significantly shorter login times on a mobile and a comparable login time on a desktop computer than text-based passwords.
Study [61]	(a) self-selection of system-generated recognition passphrase (b) system-generated recognition passphrase	- self-selection of generated system passphrase > system-generated recognition passphrase	6 words out of 20 or 100 (25.93 to 39.86 bits)	• The dictionary used contains a majority of uncommon words; thus, it is not applicable to users with different backgrounds. • The experiment was not conducted in a controlled environment such as a lab. • Typing the recognized words slightly reduces the successful login rate.
Study [19]	(a) self-selection of system-generated recognition nouns with pure recall nouns (b) self-selection of system-generated recognition passphrase with pure recall passphrase	- recognition nouns and passphrase > recall nouns and passphrase - recognition and recall passphrase > recognition and recall nouns	4 words or more out of 26 words (18.8 bits)	• The login time for noun recall is less than that for recognition. The login time for a recognition passphrase is almost similar to that for a recall passphrase. • Words with the same categorization such as "YouTube" and "Facebook" confuse users to log in successfully. • Word set with words with almost the same first letters such as "store" and "story" negatively affects the participants' retrieval of the correct password. Also, the Unmeaningful structure of passphrases has a negative impact on memorability.
Study [62]	(a) user-selection passphrase (b) conventional password	- passphrase > conventional password	4 words (crossword puzzle with 625 cells)	• Takes a long time to log in than a conventional password. • Is a complex approach and needs more training for users to accomplish the authentication process. • Is invulnerable to several attacks such as dictionary attacks, brute-force attacks, and shoulder surfing attacks.
Study [21]	system-assigned recognition (a) nouns (b) nouns with verbal cues (c) nouns with verbal and spatial cues	- nouns with verbal and spatial cues > nouns - nouns with (verbal and spatial) cues > nouns with verbal	words out of 80 (20 bits)	• The registration time for nouns with verbal and noun (spatial and verbal) cues is significantly higher than that for nouns. • The login time for nouns and nouns with (spatial and verbal) cues is significantly less than that for nouns with verbal cues. • Nouns with verbal cues have a significantly higher login rate than just nouns. • There is no significant difference in the memorability rate between nouns with verbal cues, 94.23 %, and nouns with (spatial and verbal) cues, 96.15 %.
Study [63]	system-assigned passphrases (a) CC-SP is a condition with training features (fixed location of the words, repetition, exposure time, and/or the words with semantic relations) (b) other four conditions	- CC-SP > all conditions	4 words out of 128 (28 bits)	• This study is based on Implicit learning techniques such as contextual cueing and semantic priming • CC-SP method significantly improves the usability of system-assigned passphrases, in terms of recall rates and login time. • It includes different training sessions.

cover weak password patterns, several companies have suggested password meters to determine whether the created password is strong, but the results of popular website meters have revealed many weak passwords as very strong [67]. The final goal of password meters has not comprehensively solved the problem of creating a strong password. However, a system-assigned password has been proposed as a solution to the security issue of user-chosen passwords. Different studies have reported that randomly assigned passwords are secure but difficult to remember [68]. Moreover, another study has proven a significantly low memorability rate of system-assigned passphrases than that of user-generated and mnemonic-guided passphrases [43]. A systemic review article of different composition strategies of textual passwords includes text-based, pronounceable, mnemonic, passphrase, system, and user-generated passwords; thus, user-generated passwords are more memorable than system-generated passwords [69]. Additional research attempted to reach a compromise between user-chosen and system-assigned passwords by applying a PTP approach, which requires users to select a password and then the system will perform some modifications to the actual password, as discussed in Section 2.1.5, but the study was not conducted for several sessions that evaluate the memorability rate. Overall, a recent psychological study proved that self-generated passphrases have fewer cognitive load stressors on the working memory than system-generated passphrases [70].

B. Graphical Passwords

Graphical passwords were proposed by Blonder in 1991 and are presented in a certain visual format (as opposed to the text password format). Humans remember pictures better than text, so graphical authentication passwords are possible alternatives to text-based passwords [71]. Graphical passwords have been categorized into four main schemes: drawmetric (pure-recall-based), locimetric (cued-recall-based), cognometric (recognition-based), and hybrid [72]. In general, graphical password systems have various usability and security advantages such as being easy to remember and difficult to guess, higher security level, being human-friendly, and mitigating dictionary attacks; however, they are vulnerable to shoulder-surfing attacks and brute-force attacks (which reduce the common areas in the images) [73].

1) Drawmetric (Pure-Recall-Based) and Locimetric (Cued-Recall-Based): The recall graphical password is divided into pure and cued recall-based methods [74]. The pure recall technique is called drawmetric; users generate their passwords without any clues to remember these passwords. It mainly depends on drawing a secret on a blank canvas or a grid as a simple picture, such as Draw a Secret Algorithm (DAS) Fig. 2(a) and Background Draw a Secret (BDAS) Fig. 2(b) [75]. The users must draw their secrets in an exact manner, which would require help remembering the exact stroke order [76]. These methods have a memorability range of $50\% - 80\%$ [77]; however, they have less password space and no resistance against shoulder-surfing attacks [78].

The cued-recall-based graphical password, also known as locimetric, is based on displaying an image to the users to choose different points on it [75]. The most common schemes of cued recall are blonder and pass-point. Users are required

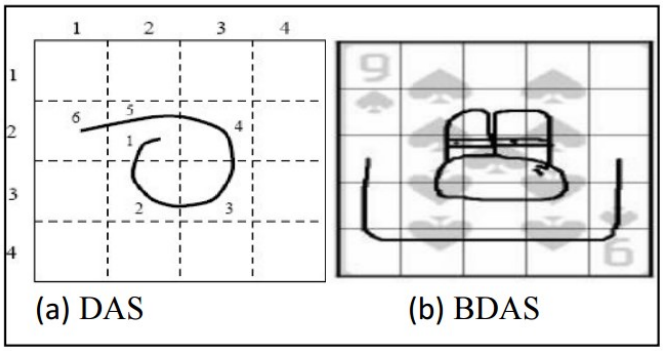

Fig. 2. Draw a secret algorithm.

in the login phase to select the same regions in a specific order, as shown in Fig. 3(a) [79]. The blonder method resists brute-force attacks because it contains millions of regions that can be selected as passwords [80]. Nevertheless, the main disadvantage of this method is that users cannot arbitrarily click on the background [78], [81]. Another mechanism called pass-point was proposed to overcome the limitation of the blonder method [82]. It allows users to select any natural image sufficiently rich to have many possible click points, which would be a hint for the users to remember their click points, as shown in Fig. 3(b) [83].

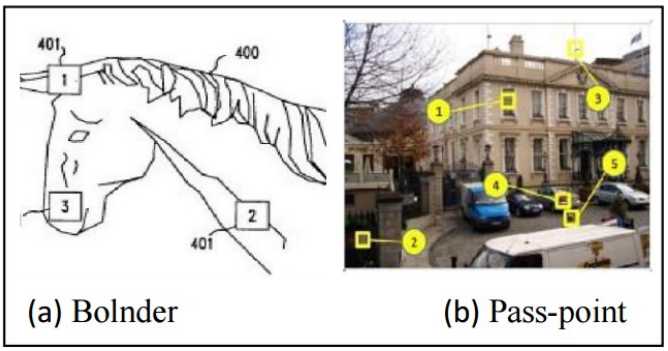

Fig. 3. Blonder and pass-point method.

2) Cognometric (recognition-based): A recognition-based graphical password scheme creates a platform for the user that contains visual passwords, and the user can select some of them as a password [18], [84]. Several image formats have been proposed for this recognition-based scheme: faces, random art pictures, icons, and daily objects [85]. Passfaces is a common method that uses human faces as a verification tool for the authentication procedure [86]. Passface is very memorable for a long period, but it is somehow predictable and vulnerable to a variety of attacks, as a majority of the users tend to select a person's face on the basis of apparent behavioral patterns, as shown in Fig. 4(a) [87]. Another version of Passface was proposed called S-Passface, which is based on replacing some characters by entering random characters corresponding to each face instead of selecting the face by the mouse, as shown in Fig. 4(b). Therefore, S-Passface is 100% resistant to shoulder surfing as compared to the original Passface version, but the security improvement has decreased

some of the usability features [88].

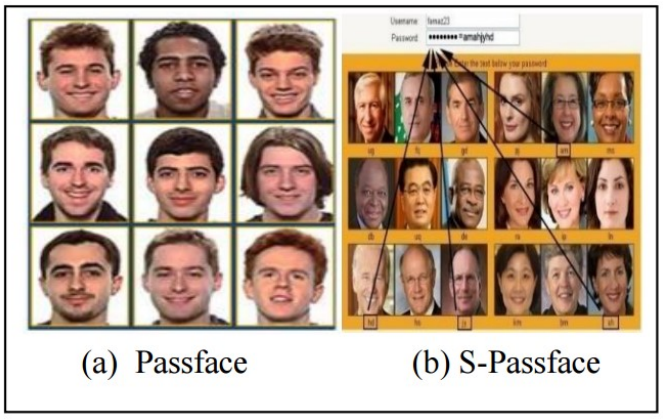

Fig. 4. Passfaces authentication systems.

Furthermore, other common recognition-based methods, Déjà Vu and story, are based on recognizing images with different principles. Déjà Vu is an algorithm that uses the technology of hash visualization of the images, as shown in Fig. 5(a) [89]. This approach showed that 90% of the participants succeeded in the authentication by using this technique, while only 70% succeeded by using text-based passwords [90]. The main disadvantage of this technique is that it takes a long time to log in because storing a large number of pictures causes a delay in transferring over the network, thus delaying the authentication process [79]. The story mechanism is comparable to the Passfaces method; it presents images of places, people, or everyday objects, as shown in Fig. 5(b). Users are instructed to mentally create linked images as a story to quickly and easily remember their passwords. The memorability result revealed that from 236 failed attempts, more than 75% were correct pictures in a wrong order [91]. Moreover, this scheme suffers from guessing and shoulder-surfing attacks [78].

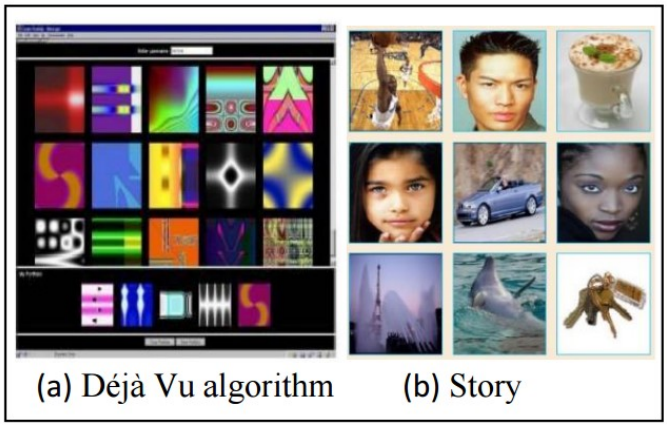

Fig. 5. Déjà Vu and story schemes.

3) Hybrid Schemes: A hybrid scheme combines two or more different types of graphical passwords or other authentication techniques for usability and security improvement [92]. According to recent studies, hybrid techniques can be classified into two categories: hybrid systems with only graphical password methods[72] and a hybrid system with a graphical and textual password [93]. Recent studies have combined recognition-based and cued-recall-based graphical passwords with images and drawn a pattern, as shown in Fig. 6(a) [94].

Moreover, the Passface scheme has been combined with traditional text passwords, as shown in Fig. 6(b) [95]. The hybrid system is utilized to overcome the limitations of graphical password schemes by creating a new system that provides a robust authentication system against spyware and shoulder-surfing attacks [96]. A recent study comprehensively deliberated hybrid graphical passwords' security levels and compared them with other graphical password systems against different attacks; thus, revealing that they had a high level of security against shoulder-surface attacks but were still vulnerable to the others [78]. However, the hybrid graphical password can provide an additional layer of security, but it could also be complex and require users to spend more time creating and entering their passwords [97]. It is critical to consider interaction while creating a hybrid graphical password system to maximize the system's effectiveness [98].

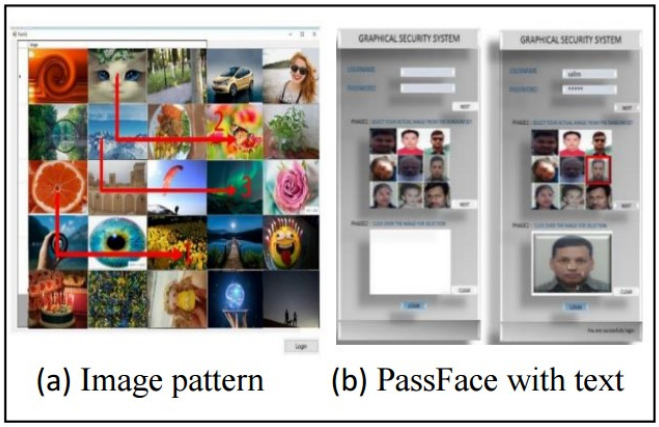

Fig. 6. Hybrid authentication system.

III. Comparative Analysis of Knowledge-based Passwords, Tokens, and Biometrics

An alternative solution has been discussed to overcome the security issue of a knowledge-based password, which are tokens and biometrics. A token password is a widely used authentication mechanism that enables users to access website resources by verifying their identity by submitting a token produced for one-time use only [99]. However, it primarily depends on third-party providers to produce tokens or one-time passwords, which makes them susceptible to the man-in-the-middle attack [100]. Moreover, researchers have reported that token passwords have a safety issue: time wastage and delays before accessing services [101]. Additionally, losing the token devices and lengthy authentication time are the main issues of this technique [102]. Thus, token passwords have a high computational cost and are expensive to implement [103].

Biometric passwords are based on people's unique behavioral and physiological characteristics and use these features as a password by using different technologies [104]. Recent studies have indicated that biometric passwords provide better

security than most of the other password types [105]. Nevertheless, biometric passwords are expensive to establish because they need high-quality devices and have a high complexity of implementation [106]. There is another concern about biometric methods, which is that no person can regulate the biometric differences caused by injury or aging [107]. The biggest security concern of biometric passwords is deceiving a security system by using copied or fake information [108]. These disadvantages of biometric methods reduce their efficiency as compared to the other types of passwords.

The knowledge-based password still provides extendable usability and security features. It can be comparable to the token and biometrics security levels with respect to mitigating most of the usability issues and security threats [1], [109]. Textual passwords are relatively still the most usable passwords because their ease of use, lack of hardware required, and less required storage [110]. A comparison of textual passwords with graphical passwords revealed a huge difference in the storage space and time consumption to login [98]. Furthermore, the shoulder-surfing attack is the most pressing security concern of graphical passwords because of their visual interface [76]. Regarding the storage problem of graphical passwords, a colored image requires a storage space of around 23.98 MB, which is significantly higher than that required by textual passwords with eight characters (57 bits) [111]. The huge size of images of graphical passwords lead to the maximization of the network latency [112]. Increasing the data transmission over the network costs more because of the complex computation and communication [113]. Furthermore, graphical passwords have an issue with communication speed as compared to textual passwords because of the picture sizes, long configuration size of registration and logging in, as well as the complexity of the encryption process [114]. Overall, graphical passwords are more expensive than textual passwords because they require large storage space to store a large number of images [115].

IV. Open Challenge and Future Trends

Authentication systems typically involve different types of credentials, such as tokens, biometrics, textual passwords, or graphical passwords. The main challenges with these systems are related to security, usability, and scalability. Each authentication method has its strengths and weaknesses, and organizations need to consider the benefits and drawbacks of each approach on the basis of their specific needs and security requirements. Biometrics and tokens offer high security, but they are costly and require particular hardware and software. Furthermore, graphical passwords require a large storage space to store large numbers of images, which causes delays in transferring the pictures over the network; therefore, they are not as widely used as textual passwords. Textual passwords are the most common type of passwords used and are regularly required to encounter certain complexity requirements. Recently, companies and government sectors (Microsoft, Canadian Government, FBI, etc.) have encouraged users to create long passphrases with the same complexity as traditional passwords to enhance security and memorability. The biggest challenge of using a long passphrase with policies as the password is the typographical errors, particularly when people need to gain experience with English as a primary language. Therefore, increasing the length of the password or passphrase helps to increase the security level, but it will make it difficult for users to login successfully. The future trend is establishing user-chosen recognition textual passwords with a high memorability rate and mitigating common attacks. This approach will be the alternated scheme for textual and graphical password schemes. It can solve several issues related to recall textual passwords such as memorization burden, lack of diversity, reuse across multiple accounts, and difficulty of password creation. Moreover, it does not require high storage space, complex implementation, and high load over the network (causing delay to login) as a graphical password scheme.

The main novelty of this paper was that specify the limitations of previous studies of recognition of textual passwords to establish a new strategy that is more competitive with other textual and graphical password, as shown in Table II. The majority of prior research on the recognition of textual passwords is based on system generated approach which results in several drawbacks. Firstly, a recent study stated that system-assigned recognition words have low memorability rates and need spatial cues (pictures) to improve word memorability; thus, they require considerable storage space, which will be costly and delay the login process [21]. Secondly, this approach needs more training to enhance password retrieval performance [63]. Finally, the word selection is limited between 4 and 5 words which cause a low password space as shown in Table II. There are different strategies that can be applied to user-chosen recognition textual passwords to enhance the usability and security level by applying a hybrid system that combines user-chosen recognition textual passwords with recall techniques or using cued recall strategies.

References

[1] M. Ali et al., "A Simple and Secure Reformation-Based Password Scheme," IEEE Access, vol. 9, pp. 11655-11674, 2021, doi:10.1109/ACCESS.2020.3049052.

[2] P. C. Golar, "An Approach Towards Usability Parameter for Graphical Based Authentication System Turkish Journal of Computer and Mathematics Education," vol. 12, no. 12, pp. 831-836, 2021.

[3] T. Haque, Md. A.; Ahmad, "'A concept of captcha based dynamic password,' Recent Advances in Computer Science and Communications, vol. 14, no. 5, pp. 1633-1640, 2021.".

[4] S. S. Almohamade, "Continuous Authentication of Users to Robotic Technologies Using Behavioural Biometrics," no. November, 2022.

[5] A. Henricks and H. Kettani, "On Data Protection Using MultiFactor Authentication," ACM International Conference Proceeding Series, no. October 2019, pp. 1-4, 2019, doi:10.1145/3394788.3394789.

[6] M. S. Kaiser, J. Xie, and V. S. Rathore, New Text-Based User Authentication Scheme Using CAPTCHA. 2023. [Online]. Available: https://app.dimensions.ai/ details/publication/pub.1148546790

[7] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, "Is FIDO2 the kingslayer of user authentication? a comparative usability study of FIDO2 passwordless authentication," Proc IEEE Symp Secur Priv, vol. 2020-May, pp. 268-285, 2020, doi:10.1109/SP40000.2020.00047.

[8] V. Zimmermann and N. Gerber, "The password is dead, long live the password - A laboratory study on user perceptions of authentication schemes," International Journal of Human Computer Studies, vol. 133, no. August 2019, pp. 26-44, 2020, doi: 10.1016/j.ijhcs.2019.08.006.

[9] M. Awad, Z. Al-Qudah, S. Idwan, and A. H. Jallad, "Password security: Password behavior analysis at a small university," International Conference on Electronic Devices, Systems, and Applications, no. May 2020, 2017, doi:10.1109/ICEDSA.2016.7818558.

[10] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," Int J Inf Secur, vol. 18 , no. 6 , pp. 741-759, 2019, doi: 10.1007/ s10207-019-00429-y.

[11] Australian Cyber Security Centre, "Creating Strong Passphrases Principles for strong passphrases Protect your passphrases Secure your passphrases," no. December 2020, pp. 1-3, 2021.
[12] Microsoft, "Create and use strong passwords," 2022. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb (accessed Sep. 07, 2022).
[13] B. Bhana and S. V. Flowerday, "Usability of the login authentication process:passphrases and passwords,"Information and Computer Security, vol. 30, no. 2, pp. 280-305,2022 , doi: 10.1108/ ICS-07-2021-0093.
[14] 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, 2021, doi: 10.1109/PST52912.2021.9647800
[15] K. Schiller and F. Adamsky, "Work in Progress: Can Johnny Encrypt E-Mails on Smartphones?," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13176 LNCS, pp. 182-193, 2022, doi: 10.1007/978-3-031-10183-0_9.
[16] E. Blanchard, "Client-Side Hashing for Efficient Typo-Tolerant Password Checkers," International Journal of Systems and Software Security and Protection, vol. 13, no. 1, pp. 1-24, 2022, doi:10.4018/ijsssp.302622.
[17] S. Sahin and F. Li, "Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication, "vol. 1, no. 1. Association for Computing Machinery, 2021. doi:10.1145/3460120.3484791.
[18] 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.
[19] 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.
[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] 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.
[22] L. Zhou, K. Wang, J. Lai, and D. Zhang, "A Comparison of a Touch-Gesture- and a KeystrokeBased Password Method: Toward Shoulder-Surfing Resistant Mobile User Authentication," IEEE Trans Hum Mach Syst, no. February, 2023, doi:10.1109/THMS.2023.3236328.
[23] R. Dillon, S. Chawla, D. Hristova, B. Gobl, and S. Jovicic, "Password policies vs. usability: When do users go 'bananas'?," Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, pp. 148-153, 2020, doi:0.1109/TrustCom50675.2020.00 032.
[24] D. Sangrey and P. Wang, "Password Change Requirements and the Effective Strength of Passwords," Issues In Information Systems, vol. 23, no. 2, pp. 29-41, 2022, doi:10.48009/2_iis_2022_103.
[25] B. Bhana and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," Comput Secur, vol. 96, p. 101925, 2020, doi:10.1016/j.cose.2020.101925.
[26] Y. Guo, Z. Zhang, Y. Guo, and X. Guo, "Nudging personalized password policies by understanding users' personality," Comput Secur, vol. 94, 2020, doi:10.1016/j.cose.2020.101801.
[27] Y. Abdrabou et al., "Your Eyes Tell You Have Used This Password Before': Identifying Password Reuse from Gaze and Keystroke Dynamics," Conference on Human Factors in Computing Systems Proceedings, no. May, 2022, doi: 10.1145/491102.3517531.
[28] B. Merdenyan and H. Petrie, "Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours," Behaviour and Information Technology, vol. 41, no. 12, pp. 2514-2527, 2022, doi: 10.1080/0144929X.2021.2019832.
[29] J.R Nirmal, R.B Kiran, and V.Hemamalini, "Improvised multifactor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics," vol. 62 , no. 7, pp. 4837-4843, 2022, doi: doi.org/10.1016/j.matpr.2022.03439.
[30] A. Nosenko, Y. Cheng, and H. Chen, "Password and Passphrase Guessing with Recurrent Neural Networks," Information Systems Frontiers, no. August, 2022, doi: 10.1007/s10796-022-10325-x.
[31] M. V. Martin, "Assessing the Memorability of Familiar Vocabulary for System Assigned Passphrases," no. August, 2021.
[32] 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.
[33] N. Jagadeesh and M. V. Martin, "Alice in Passphraseland:Assessing the Memorability of Familiar Vocabularies for System-Assigned Passphrases," arXiv, 2021.
[34] T. Pongmorrakot and R. Chatterjee, "tPAKE : Typo- Tolerant Password-Authenticated Key Exchange," International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, Cham, 2020.
[35] 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
[36] Y. Al-Slais and W. El-Medany, "User-Centric Adaptive Password Policies to Combat Password Fatigue," International Arab Journal of Information Technology, vol. 19, no. 1, pp. 55-62, 2022, doi: 10.34028/iajit/19/1/7.
[37] B. Ye, Y. Guo, L. Zhang, and X. Guo, "An empirical study of mnemonic password creation tips," Comput Secur, vol. 85, pp. 41-50, 2019, doi: 10.1016/j.cose.2019.04.009.
[38] M. Hanna, "Assisting Seniors with Technology Challenges : Video Tutorials for Password Development and Management," 2021.
[39] J. Song, D. Wang, Z. Yun, and X. Han, "Alphapwd: A Password Generation Strategy Based on Mnemonic Shape," IEEE Access, vol. 7, pp. 119052-119059, 2019, doi: 10.1109/ACCESS.2019.2937030.
[40] R. P. A. Lioy, I. Andrea, A. Candidato, and F. Sarti, "Toward a usable system-generated authentication mechanism," 2019.
[41] S. S. Woo, "How Do We Create a Fantabulous Password?," The Web Conference 2020 Proceedings of the World Wide Web Conference, WWW 2020, pp. 1491-1501, 2020, doi: 10.1145/3366423.3380222.
[42] A. M. White, K. Shaw, F. Monrose, and E. Moreton, "Isn't that Fantabulous," pp. 25-38, 2014, doi: 10.1145/2683467.2683470.
[43] S. S. Woo and J. Mirkovic, "Memorablity and Security of Different Passphrase Generation Methods," Review of KIISC, vol.28, no. 1, pp. 29-35, 2018.
[44] A. Addas, J. Thorpe, and A. SalehiAbari, "Geographic Hints for Passphrase Authentication," 2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings, 2019, doi: 10.1109/PST47121.2019.8949033
[45] A. Kanta, S. Coray, I. Coisel, and M. Scanlon, "How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts," Forensic Science International: Digital Investigation, vol. 37 , p. 301186, 2021, doi: 10.1016/j.fsidi.2021.301186.
[46] Z. Joudaki, J. Thorpe, and M. Vargas Martin, "Enhanced Tacit Secrets: System-assigned passwords you can't write down, but don't need to," Int J Inf Secur, vol. 18, no. 2, pp. 239-255, Apr. 2019, doi: 10.1007/s10207-0180408-2.
[47] K. S. Walia, S. Shenoy, and Y. Cheng, "An Empirical Analysis on the Usability and Security of Passwords," Proceedings - 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science, IRI 2020, pp. 1-8, 2020, doi: 10.1109/IRI49571.2020.00009.
[48] Y. Cheng, C. Xu, Z. Hai, and Y. Li, "DeepMnemonic: Password Mnemonic Generation via Deep Attentive Encoder-Decoder Model," IEEE Trans Dependable Secure Comput, vol. 19, no. 1, pp. 77-90, 2022, doi: 10.1109/TDSC.2020.2987025.
[49] D. He, X. Yang, B. Zhou, Y. Wu, Y. Cheng, and N. Guizani, "Password Enhancement Based on Semantic Transformation," IEEE Netw, vol. 34, no. 1, pp. 116-121, 2020, doi: 10.1109/MNET.2019.1900033.
[50] A. P. Burgoyne and R. W. Engle, "Attention Control: A Cornerstone of Higher-Order Cognition," Curr Dir Psychol Sci, vol. 29, no. 6, pp. 624-630, 2020, doi: 10.1177/0963721420969371.
[51] H. Feng, "Memory studies of chunking and decay of memory," vol. 36, pp. 709-714, 2023.
[52] D. Ševerdija, "Working Memory in Word Recall," pp. 2-29, 2023, [Online]. Available: https://urn.nsk.hr/urn:nbn:hr:13 1:382156
[53] W. Xie, W. A. Bainbridge, S. K. Inati, C. I. Baker, and K. A. Zaghloul, "Memorability of words in arbitrary verbal associations modulates memory retrieval in the anterior temporal lobe," Nat Hum Behav, vol. 4, no. 9, pp. 937-948, 2020.
[54] V. Popov and L. Reder, "Frequency effects in recognition and recall," Handbook of Human Memory, pp. 1-31, 2021.
[55] J. Verhagen, M. van Stiphout, and E. Blom, "Determinants of early lexical acquisition: Effects of word- and child-level factors on Dutch

children's acquisition of words," J Child Lang, vol. 49, no. 6, pp. 1193-1213, 2022, doi: 10.1017/SO305000921000635.

[56] M. Ponari, C. Frazier Norbury, and G. Vigliocco, "The role of emotional valence in learning novel abstract concepts Marta Ponari," Dev Psychol, vol. 56, no. 10, pp. 1855-1865, 2020.

[57] J. Kaleńska-Rodzaj, "Preperformance emotions and music performance anxiety beliefs in young musicians," Research Studies in Music Education, vol. 42, no. 1, pp. 77-93, 2020, doi: 10.1177/1321103 × 19830098.

[58] S. M. Mohammad, "Obtaining reliable human ratings of valence, arousal, and dominance for 20,000 English words," ACL 2018 56th Annual Meeting of the Association for Computational Linguistics, Proceedings of the Conference (Long Papers), vol. 1, pp. 174-184, 2018, doi: 10.18653/v1/p18 − 1017.

[59] A. Jha, K. R. Bhatele, P. Philip, and K. Mishra, "Graphical Password Authentication System for Web and Mobile Applications in JavaScript," pp. 160-185, 2022, doi: 10.4018/978-1-6684-58273.ch011.

[60] 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 (MoST 13), 2013.

[61] N. K. Blanchard, C. Malaingre, and T. Selker, "Improving security and usability of passphrases with guided word choice," pp. 723732, 2018, doi: 10.1145/3274694.3274734.

[62] B. B. B. and T. T. H. Tazawa, T. Katoh, "A user authenticaion scheme using multiple passphrases and its arrangement," 2010.

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

[64] U. Farooq, "Real Time Password Strength Analysis on a Web Application Using Multiple Machine Learning Approaches," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 12, pp. 359-364, 2020.

[65] D. K. Davis, M. M. Chowdhury, and N. Rifat, "Password Security: What Are We Doing Wrong?," IEEE International Conference on Electro Information Technology, vol. 2022-May, pp. 562-567, 2022, doi: 10.1109/eIT53891.2022.9814059.

[66] R. Alomari, M. V. Martin, S. MacDonald, A. Maraj, R. Liscano, and C. Bellman, "Inside out - A study of users' perceptions of password memorability and recall," Journal of Information Security and Applications, vol. 47, pp. 223-234, 2019, doi: 10.1016/j.jisa.2019.05.009.

[67] J. M. Pittman and N. Robinson, "Shades of Perception- User Factors in Identifying Password Strength," 2020, [Online]. Available: http://arxiv.org/abs/2001.04930

[68] J. Kävrestad, M. Lennartsson, M. Birath, and M. Nohlberg, "Constructing secure and memorable passwords," Information and Computer Security, vol. 28, no. 5, pp. 701717, 2020, doi: 10.1108/ICS-072019-0077.

[69] M. Lennartsson, "Evaluating the Memorability of Different Password Creation Strategies: A Systematic Literature Review," 2019.

[70] 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.

[71] T. Khodadadi, Y. Javadianasl, F. Rabiei, M. Alizadeh, M. Zamani, and S. S. Chaeikar, "A Novel Graphical Password Authentication Scheme with Improved Usability," 2021 4th International Symposium on Advanced Electrical and Communication Technologies, ISAECT 2021, no. December, 2021, doi: 10.1109/ISAECT53699.2021.9668 599.

[72] S. Z. Nizamani, S. R. Hassan, R. A. Shaikh, E. A. Abozinadah, and R. Mehmood, "A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability," IEEE Access, vol. 9, pp. 51294-51312, 2021, doi: 10.1109/ACCESS.2021.3069164.

[73] S. W. Jirjees, A. M. Mahmood, and A. R. Nasser, "Passnumbers: An Approach of Graphical Password Authentication Based on Grid Selection," International Journal of Safety and Security Engineering, vol. 12, no. 1, pp. 21-29, 2022, doi: 10.18280/ijsse.120103.

[74] K.Lapin and M.Šiurkus, "Balancing Usability and Security of Graphical Passwords," vol. 440. 2022. [Online]. Available: https://link.springer.com/10.100 7/978-3-031-11432-8

[75] A. Khan and A. G. Chefranov, "A Captcha-Based Graphical Password with Strong Password Space and Usability Study," 2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, no. June, pp. 12-13, 2020, doi: 10.1109/ICECCE49384.2020.9179 265.

[76] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical User Authentication System Resistant to Shoulder Surfing Attack," Adv Res, vol. 19, no. 4, pp. 1-8, 2019, doi: 10.9734/air/2019/v19i430126.

[77] B. Robert, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput Surv, vol. 44, no. 4, pp. 1-41, 2012, doi: 10.1145/2333112.2333114.

[78] T. I. Shammee, T. Akter, M. Mou, F. Chowdhury, and M. S. Ferdous, "A Systematic Literature Review of Graphical Password Schemes," Journal of Computing Science and Engineering, vol. 16, no. 4, pp. 163-185, 2020, doi: 10.5626/JCSE.2020.14.4.163.

[79] F. Ghiyamipour, "Secure graphical password based on cued click points using fuzzy logic," Security and Privacy, vol. 4, no. 2, pp. 1− 26, 2021, doi: 10.1002/spy2.140.

[80] A. F. MUAFIAH, "A Secure Shoulder Surfing Resistant Hybrid Graphical User Authentication Scheme," Ayan, vol. 8, no. 5, p. 55, 2019.

[81] N. A. Bi. M. Fazil, "Graphical Password Authentication Using Cued Click Point Technique," Universiti Sultan Zainal Abidin, 2021.

[82] I. Journal, O. F. Advance, and E. Trends, "Graphical Systems Authentication Using Ascii," vol. 4, no. 6, pp. 24-30, 2020.

[83] J. A. Herrera-macías, C. M. Legónpérez, L. Suárez-plasencia, L. R. Piñeiro-díaz, O. Rojas, and G. Sosa-gómez, "SS symmetry Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points †," pp. 1-19, 2021.

[84] J. G. Kaka and O. J. O, "Recognition Based Graphical Password Algorithms: A Survey," 2021.

[85] P. U. Gujare, A. S. Kapse, and A. S. Kapse, "Three way authentication technique using User Defined Graphical Authentication System," vol. 5, no. 6, pp. 185188, 2020.

[86] Prof. P. S. Gayke, Shraddha Thorat, Gayatri Nagarkar, Priyanka Kusalkar, and Priyanka Waditake, "Secure Data Access using Steganography and Image Based Password," Int J Sci Res Sci Technol, pp. 193-198, 2022, doi: 10.32628/ijsrst229343.

[87] U. Bedekar and G. Bhatia, "A Novel Approach to Recommend Skincare Products Using Text Analysis of Product Reviews", vol. 191, no. Ictcs. 2022. doi: 10.1007/978-981-16-0739-4_24.

[88] P. Jittibumrungrak and N. Hongwarittorrn, "A preliminary study to evaluate graphical passwords for older adults," ACM International Conference Proceeding Series, pp. 88-95, 2019, doi: 10.1145/3328243.3328255.

[89] H. U. Suru, A. A. Muslim, S. U. Suru, and H. U. Suru, "A Review of Graphical, Hybrid and Multifactor Authentication Systems," vol. 10, no. 1, pp. 1447-1475, 2019.

[90] H. Umar Suru and P. Murano, "Security and User Interface Usability of Graphical Authentication Systems - A Review," International Journal of Computer Trends and Technology, vol. 67, no. 2, pp. 17-36, 2019, doi: 10.14445/22312803/ ijcttv67i2p104.

[91] H. M. Aljahdali and R. Poet, "The affect of familiarity on the usability of recognition-based graphical passwords: Cross cultural study between Saudi Arabia and the United Kingdom," Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, pp. 1528-1534, 2013, doi: 10.1109/TrustCom.2013.187.

[92] N. Kausar, I. U. Din, M. A. Khan, A. Almogren, and B. S. Kim, "GRAPIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices," Sensors, vol. 22 , no. 4, pp. 1-17, 2022, doi: 10.3390/s22041349.

[93] B. Sharma, S. S. Patel, A. Jaiswal, and Y. Arora, "Hybrid Graphical Password Auhtentication System," no. 02, pp. 113-118, 2021.

[94] F. Sepideh, "Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing , Smudge and Brute Force Attack," vol. 13 , no. 12 , pp. 624-628, 2019.

[95] S. Istyaq, A. Nazir, and M. S. Umar, "Hybrid Graphical User Authentication Scheme Using Grid Code," Int. j. eng. trends technol., vol. 69, no. 5, pp. 166176, 2022, doi: 10.14445/22315381/IJETT- V69I5P223.

[96] M. Elhoseny and A. K. Singh, "Smart Network Inspired Paradigm and Approaches in IoT Applications", 1st ed. Singapore: Singapore: Springer, 2020.

[97] S. S. Patel, A. Jaiswal, Y. Arora, and B. Sharma, "Survey on Graphical Password Authentication System," pp. 699708, 2021, doi: 10.1007/978-98115-8530-2_55.

[98] G. C. Yang, "Development status and prospects of graphical password authentication system in Korea," KSII Transactions on Internet and Information Systems, vol. 13, no. 11, pp. 5755-5772, 2019, doi: 10.3837/tiis.2019.11.026.

[99] Y. Zhang, C. Xu, H. Li, K. Yang, N. Cheng, and X. Shen, "PROTECT:

Efficient Password-Based Threshold Single-Sign-On Authentication for Mobile Users against Perpetual Leakage," IEEE Trans Mob Comput, vol. 20, no. 6, pp. 2297-2312, 2021, doi: 10.1109/TMC.2020.2975792.

[100] R. H. Khan and J. Miah, "Performance Evaluation of a new one-Time password (OTP) scheme using stochastic petri net (SPN)," 2022 IEEE World AI IOT Congress, AlloT 2022, no. August, pp. 407-412, 2022, doi: 10.1109/AlloT54504.2022.98172 3.

[101] M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Improved Time-Based One Time Password Authentication Framework for Electronic Payments," International Journal of Advanced Computer Science and Applications, vol. 11, no. 11, pp. 359-366, 2020, doi: 10.14569/IJACSA.2020.0111146.

[102] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth, "'You still use the password after all' - Exploring FIDO2 Security Keys in a Small Company," Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020, pp. 19-36, 2020.

[103] S. Sudha and S. S. Manikandasaran, "Asynchronous Password-Based Authentication and Service_Provider_ID Module for Secured Cloud Environment," International Journal of Computer Theory and Engineering, vol. 12, no. 4, pp. 85-91, 2020, doi: 10.7763/ijcte.2020.v12.1269.

[104] I. Alsaadi and I. Majeed Alsaadi, "Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review," International Journal of Scientific & Technology Research, vol. 10, no. January, p. 1, 2021, doi: 10.13140/RG.2.2.28802.09926.

[105] C. Lipps, J. Herbst, and H. D. Schotten, "How to Dance your Passwords: A Biometric MFA- scheme for Identification and Authentication of Individuals in IIoT Environments," Proceedings of the 16th International Conference on Cyber Warfare and Security. International Conference on Cyber Warfare and Security (ICCWS-2021), February 25-26, Cookeville,, Tennessee, USA, 2021, doi: 10.34190/IWS.21.016.

[106] N. A. K. Abiew, M. D. Jnr., and S. O. Banning, "Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems," Asian Journal of Research in Computer Science, no. April, pp. 7-20, 2020, doi: $10.9734/\mathrm{ajrcos}/2020/v5i330135$.

[107] M. Akbari, "A Multimodalbiometric Identi cation System Based on Deep Features to Identify Individuals," 2022.

[108] D. M. Omarova and I. S. Mutayeva, "BIOMETRICS AS A METHOD OF COMBAT WITH COVID-19," in Smart Innovation, Systems and Technologies, International scientific conference, 2020.

[109] M. Wanuna, "Dynamic knowledge based authentication model for enhancing security of USSD banking transactions," 2020, [Online]. Available: http://hdl.handle.net/11071/120 89Followthisandadditionalworksat:http://hdl.handle.net/11071/12 089

[110] M. Ahsan and Y. Li, "Graphical Password Authentication using Images Sequence," International Research Journal of Engineering and Technology, vol. 9001, p. 1824, 2008, [Online]. Available: www.irjet.net

[111] Pankhuri, A. Sinha, G. Shrivastava, and P. Kumar, "A pattern-based multi-factor authentication system," Scalable Computing, vol. 20, no. 1, pp. 101-112, 2019, doi: 10.12694/scpe.v20i1.1460.

[112] O. N. Toxirjonovich, A. A. Xusnidinovich, and A. U. Y. O'g'li, "Multi-factor Authentication System Based on Template," JournalNX, vol. 7, no. 05, pp. 4960, 2021.

[113] 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, 2019, doi: 10.1007/s11036-019-01252-4.

[114] B. Yao, Y. Mu, H. Sun, X. Zhang, H. Wang, and J. Su, "Connection between text-based passwords and topological graphic passwords," Proceedings of 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference, ITOEC 2018, no. Itoec, pp. 1090-1096, 2018, doi: 10.1109/ITOEC.2018.8740702.

[115] B. Rasmussen and D. Zapppala, "A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement," ProQuest Dissertations and Theses, p. 36, 2021, [Online]. Available: https://www.proquest.com/dissertations theses/usability-studyfido2-roaming-software-tokens as/docview/2600829489/se- 2?accountid = 202211%0 https://media.proquest.com/media/hms/PFT/2/RrxJL?_a=ChgyMD IyMDUyMDA4MjcyNjExNDo1ODkyMzISBzEzODc5ODEaCk9ORV9TRUFSQ0giD