SCIENTIFIC Publishing Limited

Journal of Intelligent Communication
https://ojs.ukscip.com/index.php/jic

Review

A Systematic Review of Cognitive Passwords: Limitations, Challenges, and Solutions

Mohammed Sharaf Alwajeeh [1,*], Mubarak Mohammed Al-Ezzi Sufyan [2], Mokhtar H. Al-Sarori [1], Mahfoudh Al-Asaly [3] and Ghassan Abdullah Abdulwasea Al-Maamari [1]

[1] Faculty of Information Technology and Computer Science, University of Saba Region, Marib, Yemen
[2] Department of Computer Information Systems, Al-Jawf Faculty, University of Saba Region, Marib, Yemen
[3] Department of Information Technology, College of Computer, Qassim University, Buraydah 51174, Saudi Arabia
[*] Correspondence: mohammedsharaf32@gmail.com

Received: 12 October 2025; **Revised:** 20 November 2025; **Accepted:** 28 November 2025; **Published:** 12 December 2025

Abstract: This study provides a comprehensive analysis of cognitive password systems as a secure and user-friendly alternative to traditional authentication mechanisms. Cognitive passwords leverage human memory, behavior, and perception to enhance usability while mitigating common security challenges such as poor memorability, password reuse, and susceptibility to attacks. The study systematically reviews various models, including graphical passwords, cognitive biometrics, and cognitive one-time passwords (OTPs), highlighting their strengths and limitations. To ensure a transparent and rigorous review, we employed a structured methodology comprising a multi-database literature search, clearly defined inclusion and exclusion criteria, and a thematic synthesis of the collected studies. Our findings indicate that cognitive password systems offer significant improvements in user experience and security but face critical challenges, including accessibility for individuals with cognitive or physical impairments, privacy concerns, vulnerability to social engineering, and scalability limitations. Furthermore, artificial intelligence (AI) emerges as a key enabler for enhancing personalization, adaptive authentication, and real-time security risk assessment. The study underscores the necessity of integrating AI thoughtfully to maximize the benefits of cognitive passwords. Overall, this research demonstrates the transformative potential of cognitive password systems in cybersecurity, emphasizing that addressing usability, privacy, and scalability challenges is essential for their practical adoption. The findings provide actionable insights for system designers, policymakers, and researchers aiming to advance secure and user-centered authentication frameworks.

Keywords: Cognitive; Password; Security; Usability; Biometric; Authentication

1. Introduction

Cognitive passwords offer a user-centric authentication method based on personal memories, experiences, or facts, making them inherently more memorable and secure compared to traditional character-based passwords. Originating in the 1990s as a response to escalating vulnerabilities in conventional password systems, the concept gained traction with the pioneering work of Dias and Reeja, Palmgren and Byström [1,2], who proposed cognitive authentication schemes as a replacement for traditional passwords [1,2]. These systems leverage cognitive science to align password creation with human memory capabilities, thereby enhancing usability and reducing susceptibility to attacks such as phishing and password cracking. Approaches include using narrative elements, cognitive one-time passwords (OTP), and augmented cognition to minimize cognitive load while maintaining robust security [2,3]. The ini-

https://doi.org/10.54963/jic.v5i1.1697

tial implementation of cognitive password systems, notably the "Pass Thoughts" model, authenticated users through a combination of personal memories, facts, and experiences [4,5]. By prompting users with questions about their history, preferences, and interests, the system generated a unique authentication token, enhancing both security and user-friendliness. Since then, cognitive authentication has evolved significantly, integrating advanced technologies such as machine learning and natural language processing to optimize both usability and resistance to attacks. In this context, this study categorizes research on cognitive passwords based on limitations, challenges, and proposed solutions as the main idea, as shown in **Figure 1**.

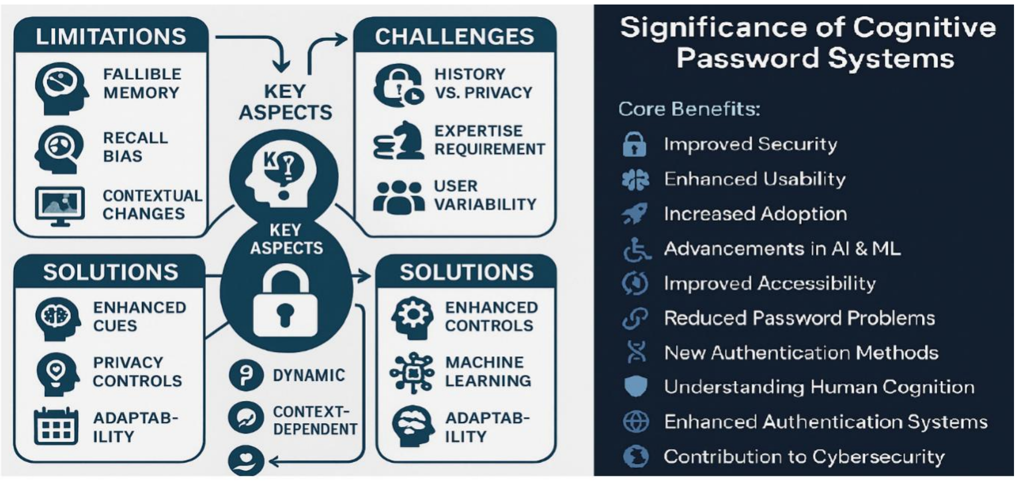

Figure 1. The main idea of this comprehensive study.

Despite the innovative nature of cognitive password systems, they face several persistent challenges, such as usability difficulties, cognitive overload, limited user adoption, and vulnerability to behavioral and pattern-based attacks. Furthermore, existing research on these systems remains fragmented, lacking comprehensive reviews of core concepts, methodologies, and performance metrics, which hinder a comprehensive understanding of emerging trends and critical research gaps [6]. Studies reveal that many users reuse a limited set of passwords across accounts, heightening vulnerability and emphasizing the necessity for improved authentication solutions and password management tools [7]. Research also indicates that weaker passwords at lower security levels can compromise stronger ones, highlighting the importance of maintaining distinct, robust credentials, especially for protecting vulnerable populations such as children [8,9]. The prevalent use of simple, easy-to-remember passwords, and password reuse across multiple accounts, poses significant security risks, as users' credentials are often predictable and easily compromised [10]. Alternative methods like biometrics and token-based systems have been explored but encounter challenges related to usability, security, and privacy [11]. To address memory-related challenges, studies have demonstrated that strategies leveraging long-term memory, such as list reduction techniques, can significantly improve users' ability to recall multiple passwords, balancing strength and memorability [12]. Understanding human memory's role in password security is vital, with research proposing new and revised memory theories to enhance password memorability without compromising security [13]. Cognitive password authentication emerges as a promising approach by utilizing users' cognitive abilities for identity verification. This method is particularly significant for securing personal information and online data, as highlighted in recent cybersecurity research [14].

By conducting a comprehensive study of the limitations, challenges, and solutions of cognitive passwords, this study aims to contribute to the development of more secure, user-friendly, and privacy-preserving authentication systems, ultimately enhancing the security and trust of online systems/environments. This motivated us to conduct this comprehensive study to achieve the main aims of this study, as investigate the potential of cognitive password authentication, to study and evaluate a cognitive password authentication system by addressing the limitations of password-based methods, and how they can be used to improve, and enhance the security and usability through the application of cognitive principles and innovative technologies. This will be accomplished by achieving the following objectives: To provide a comprehensive review of the existing literature on cognitive passwords, systematically summarizing key concepts, methodologies, and research findings, and to identify and categorize the current limitations of cognitive password systems, which will encourage researchers to address unresolved challenges and inform future research efforts. Additionally, to highlights areas that require further exploration and outlines emerging trends and potential research directions for scholars. Moreover, this work aims to present and discuss the common performance metrics used to evaluate the effectiveness of cognitive password systems, such as security, usability, memorability, uniqueness, password strength, and efficiency. Furthermore, the study proposes a theoretical framework to underpin cognitive passwords, demonstrating their potential to enable more flexible, intelligent, and scalable systems. The broader implications of this integration are assessed across various domains. The methodology involved a structured review of contemporary academic literature, industry reports, and emerging technology trends. A thematic synthesis approach was employed to systematically extract and categorize recurring challenges, opportunities, and ethical considerations. Comparative analysis with current systems implementations was conducted to assess technological maturity and identify research gaps, ensuring a well-rounded perspective on both technical and societal dimensions. The key contributions of this study are as follows:

1. Identification of Optimal Question Types and Difficulty Levels: We contributed to the development of cognitive password systems by identifying the optimal question types and difficulty levels that balance security and usability.
2. Investigation of Privacy Implications and Mitigation Strategies: We investigate the potential privacy implications of cognitive password systems and provide recommendations for mitigating these risks.
3. Empirical Evaluation of Cognitive Password Systems: We contribute to the empirical evaluation of cognitive password systems, providing insights into their security, usability, and effectiveness.
4. Best Practices for Implementing Cognitive Password Systems: We provide best practices for implementing cognitive password systems, including guidelines for question design, user enrollment, and system maintenance.

This article is organized as follows: Sections 2 discuss the methodology of the review while section 3 cover the cognitive password work. Sections 4 to 7 discuss challenges and limitations of cognitive passwords their role in cybersecurity, AI, and Existing Solutions. Sections 8 and 9 present the cognitive password system and discussion. Finally, Sections 10 address the Challenges, Open Issues, and Recommendations for Cognitive Password Systems follow by conclusion in section 10.

2. Methodology

This study adopts a Systematic Literature Review (SLR) methodology, which is well-suited for examining cognitive passwords. The approach enables a structured investigation of the limitations, challenges, usability considerations, and security aspects of cognitive authentication, while also identifying research gaps and potential directions for future studies [1,3,6,15,16]. To visualize the selection process, a PRISMA flow diagram was employed, which includes three primary stages: identification, screening, and inclusion. The review considers publications from 2013 to 2025 to ensure coverage of recent developments in cognitive password research.

The identification phase involved applying filters for publication date, type (journal articles, conference proceedings, books), and relevance to the topic, thereby excluding duplicates and non-conforming records. During the screening phase, shortlisted studies were evaluated based on thematic relevance, methodological rigor, and depth of contribution. Articles that did not meet these criteria were excluded. The inclusion phase produced the final corpus of literature that forms the basis of this review [2,4,5,7,10,12].

Systematic Search Protocol: The review employed targeted keywords and search strings to capture relevant studies in the areas of cognitive passwords, authentication, usability, human-computer interaction, and security. Boolean operators (e.g., AND, OR) were used to refine searches. Examples of search strings include:

("cognitive passwords" OR "password security") AND ("usability" OR "human-computer interaction"). This strategy ensured the retrieval of studies addressing both security and usability aspects of cognitive authentication [8,14,17–20].

Data Sources: The systematic search was conducted across major scholarly databases and digital libraries, including Google Scholar, IEEE Xplore, ACM Digital Library, Scopus, Web of Science, SpringerLink, and Elsevier.

These sources were selected for their high-quality, peer-reviewed publications relevant to cybersecurity, usability, and cognitive authentication research [9,11,21–23].

Selection and Screening: Initial screening involved evaluating titles and abstracts for relevance. Studies passing this stage underwent a full-text review to assess methodological rigor and alignment with the inclusion criteria. The complete paper selection process is illustrated in **Figure 2**, which follows the PRISMA framework. This systematic procedure ensures the inclusion of studies that provide robust empirical evidence, theoretical insights, and practical considerations in cognitive password research [24–28].

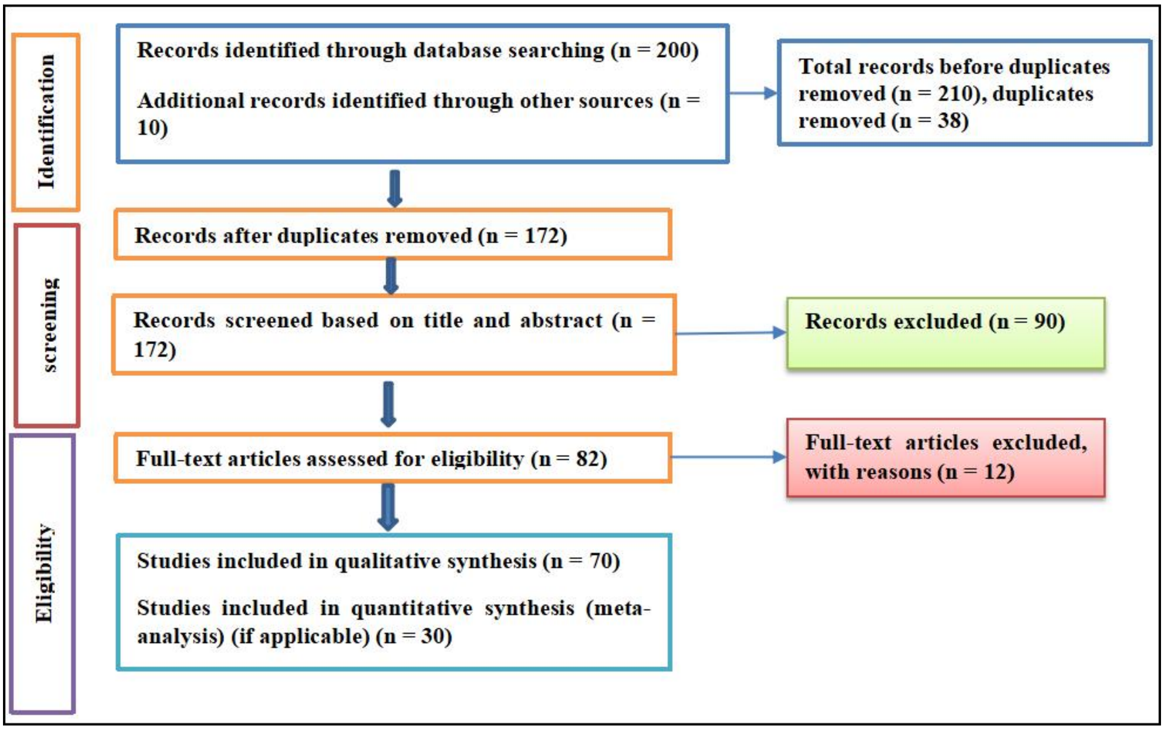
Identification
Records identified through database searching (n = 200)
Additional records identified through other sources (n = 10)
Total records before duplicates removed (n = 210), duplicates removed (n = 38)
screening
Records after duplicates removed (n = 172)
Records screened based on title and abstract (n = 172)
Records excluded (n = 90)
Full-text articles assessed for eligibility (n = 82)
Full-text articles excluded, with reasons (n = 12)
Eligibility
Studies included in qualitative synthesis (n = 70)
Studies included in quantitative synthesis (meta-analysis) (if applicable) (n = 30)

Figure 2. Selecting papers for a systematic review using the PRISMA framework.

3. How Cognitive Passwords Work?

Cognitive passwords authenticate users by leveraging personal facts, memories, and experiences through various question types. These include personal history-based questions (e.g., birthdate or significant life events), knowledge-based questions (e.g., favorite books or sports teams), and behavioral questions (e.g., daily routines or hobbies) [15]. Numerous methods have been proposed to strengthen privacy, integrity, and authentication in cognitive password systems, underscoring their significance for both individuals and organizational information systems. Despite the growing need for secure and user-friendly authentication, password-based systems remain ubiquitous due to their integration into most digital services. However, the rapid increase in password use leads to low-entropy choices and password fatigue, often exacerbated by complex password policies that users find difficult to comply with, sometimes resorting to insecure practices like writing passwords down [8,9,24]. Alternatives such as biometric authentication, two-factor authentication, and graphical passwords have been developed to overcome these issues. Biometrics offer convenience and security by using unique physical traits, while two-factor authentication combines multiple verification elements. Graphical passwords leverage ease of memory through visual cues. However, the widespread replacement of traditional password systems faces challenges due to legacy infrastructure and slow adoption rates, which act as significant barriers to their mass implementation [10]. **Figure 3** illustrates this working mechanism.

This study addresses several key questions regarding cognitive passwords, including: how to design systems that balance security and usability? How to optimize question types and difficulty levels for enhanced performance? how to integrate cognitive passwords with multi-factor authentication for stronger security; and how to identify and mitigate potential privacy concerns. Accordingly, this comprehensive research aims to answer: How can cognitive password systems be both secure and user-friendly? What are the best question types and difficulty settings? How can these systems be combined with other authentication methods? And how can privacy risks be effectively managed?

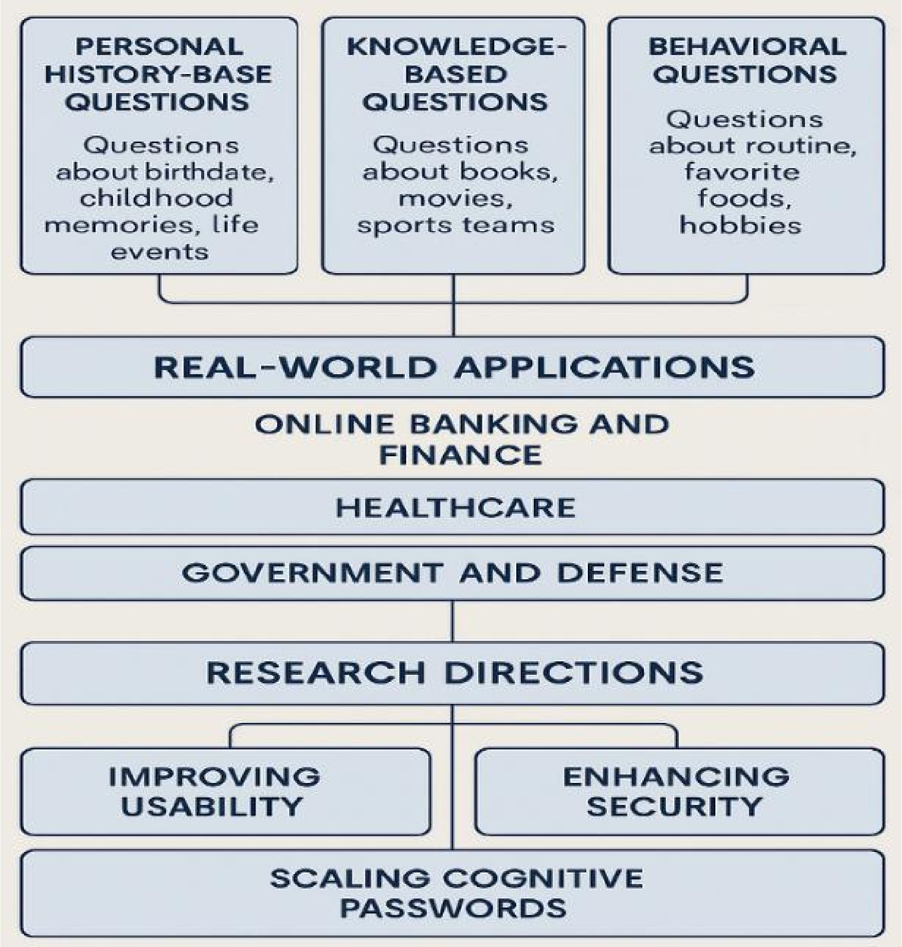
PERSONAL HISTORY-BASE QUESTIONS
Questions about birthdate, childhood memories, life events
KNOWLEDGE-BASED QUESTIONS
Questions about books, movies, sports teams
BEHAVIORAL QUESTIONS
Questions about routine, favorite foods, hobbies
REAL-WORLD APPLICATIONS
ONLINE BANKING AND FINANCE
HEALTHCARE
GOVERNMENT AND DEFENSE
RESEARCH DIRECTIONS
IMPROVING USABILITY
ENHANCING SECURITY
SCALING COGNITIVE PASSWORDS

Figure 3. How Cognitive Passwords Work?

4. Challenges and Limitations of Cognitive Passwords

While cognitive passwords offer several advantages, they also present several challenges and limitations, including:

4.1. Cognitive Passwords for Usability

This section reviews key research on cognitive password authentication, focusing on usability challenges and cognitive principles. This principle of usability extends to authentication design, as users often prioritize security over usability, adopting various strategies to balance protection and convenience when creating passwords [29]. For instance, poor usability of security-related APIs, especially cryptographic ones, often leads to developer errors and security risks. Improving these APIs' usability is critical [30]. In addition, password managers reduce cognitive effort and simplify authentication over time, as revealed by a study investigating their usability for novice users when they handle more accounts [21]. Cognitive password systems, especially those using graphical elements and passphrases, leverage human cognitive strengths like visual memory and associative recall to enhance usability without compromising security. For instance, Al-Ameen et al. [17] demonstrated effective password recall using combined visual, verbal, and spatial cues. Graphical password models compliant with ISO usability standards have shown high user satisfaction [31], and personalization based on user cognition influences password preference [22]. Systems such as CAPTCHA-based and grid-based graphical passwords improve memorability and resist attacks like shoulder surfing [18,32]. However, hybrid models combining textual and graphical passwords may sometimes offer better usability [33]. Behavior-based approaches, like handwriting biometrics [23] and steganography-embedded QR codes [34], also reduce cognitive load. Inclusive design addressing cognitive disabilities is essential for equitable usability [19]. Overall, cognitive password systems that incorporate visual, behavioral, and personalized elements significantly improve security and user experience. **Table 1** summarizes these contributions.

Table 1. Summary of Existing Research on Cognitive Passwords for Usability.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Wijayarathna et al. [30]	Usability in cryptographic APIs	SCrypt in Bouncycastle API	Identified 63 issues, improving API design	Feedback from 10 programmers	Better API usability reduces errors and vulnerabilities
Al-Ameen et al. [17]	Password recall and security	Visual, verbal, and spatial cues	Improved recall within 3 attempts after 1 week	Recall success rate	Cognitive cues enhance password recall and security
Sarkhoshi et al. [31]	Usability of graphical passwords	ISO-aligned cognitive model	Validated usability and acceptance	User questionnaires	Cognitive graphical passwords improve user experience
Loos et al. [22]	Memory and passphrase recall	Associative memory factors	Found variation by cognitive control type	Recall rates and feedback	Memory associations are key to passphrase usability
Naik et al.[18]	Password complexity	Images, shapes, and patterns	Simplified recall with visuals	User feedback	Visual cues reduce complexity and improve usability
Lapin et al. [32]	Balancing usability and security	Visual memory–based graphical passwords	Lowered cognitive load and shoulder-surfing risk	Usability & security tests	Graphical methods enhance both security and usability
Patil et al. [33]	Graphical password usability	Hybrid cognitive-graphical system	Proposed effective hybrid solution	User evaluations	Hybrid model improves authentication usability
Contreras [23]	Authentication uniqueness	Writing-style cognitive system	Secure login via handwriting traits	User feedback	Writing-based login improves usability and security
Balayogi et al. [34]	Password management burden	MASTER with QR and steganography	Centralized and simplified access	SUS score: 75.94	MASTER reduces cognitive effort and enhances usability
Kävrestad et al. [19]	Accessibility for cognitive disabilities	Inclusive design guidelines	Improved support for diverse users	Design evaluation	Adapting to cognitive needs improves usability
Krzyworzeka et al. [35]	Password memorability	CAPTCHA with personalized images	Enhanced recall and security	User recall feedback	Personalized CAPTCHA boosts usability and security
Khan et al. [36]	Traditional password issues	CODP and COSS schemes	Improved usability via recognition & recall	User evaluation	Graphical schemes outperform text passwords

4.2. Cognitive Password for Security

This section critically reviews recent advancements in cognitive password systems that leverage human cognitive abilities to enhance authentication. These systems improve memorability and security by integrating user knowledge, memory, and perception. Cognitive one-time passwords (OTPs) generate personalized security questions, reducing unauthorized access risks [37]. Visual modifications to password characters aid recall and discourage insecure behaviors [38], while cognitive CAPTCHAs require specialized knowledge, supporting expert-level access control [25]. Personalized authentication models use familiar images and cues to simplify managing multiple passwords [39,40]. Moreover, personality traits and cognitive factors significantly influence individuals' password security behaviors [26]. In this regard, the challenges such as cognitive overload and accessibility have been addressed through cognitive load theory applied in training [41] and eye-tracking studies linking mental effort with password strength [42]. Extensions include multi-platform cognitive OTPs [37], multilevel cryptographic authentication for cloud security [25], and adaptive systems assisting users after failed login attempts [40]. Narrative-based passwords and association-based memorization improve recall and resist attacks [43,44], complemented by behavioral password-strength evaluations [20]. Cognitive sequences during login embed additional security layers [45,46]. Overall, cognitive password systems advance security and usability, with ongoing research focusing on personalization and adaptability. **Table 2** summarizes these findings.

Table 2. Summary of the existing works in cognitive password for Security.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Grunin et al. [37]	Static password weaknesses	Cognitive OTPs using dynamic user-specific questions	Enhanced password uniqueness and contextual security	User feedback, security analysis	Personalized OTPs improve dynamic security
Mogire et al. [38]	Recall difficulty & insecure habits	Cognitive transformations (e.g., font, weight)	Reduced cognitive effort and discouraged risky behaviors	Recall rates, user response	Visual cues aid memory and support secure practices
Ogiela [25]	Secure password management for cloud	Cognitive cryptographic methods	Strengthened cloud password systems	Usability, security tests	Cognition-driven methods enhance password security
Krzyworzeka et al. [39]	Multi-password overload	Familiar images & personal cues	Simplified recall with strong personalized security	User/system feedback	Personalized cues ease password management
Deluca et al. [40]	Usability during failed logins	Failure monitoring with guidance prompts	Improved login experience and system responsiveness	System/user feedback	Adaptive systems enhance trust and usability
Abdrabou et al. [42]	High mental effort in password creation	Eye-tracking pupil dilation analysis	Linked stronger passwords with increased cognitive load	Pupil data, strength scores	Cognitive effort predicts password quality
Hoover et al. [43]	Brute-force and guessable passwords	Narrative-based cognitive passwords	Improved memorability using story elements	Usability, attack resistance	Story-based passwords reduce predictability
Khare et al. [44]	Shoulder surfing threats	Association-based memory techniques	Protected passwords from visual theft	Security/usability analysis	Cognitive memory defends against observation attacks
Goldberg et al. [20]	Weak and repetitive password habits	Analysis of keyboard use patterns	Detected insecure typing behaviors	Behavior tracking, user analysis	Pattern recognition improves user awareness
Ogiela et al. [45]	Lack of cognitive challenge in login	Visual path-based authentication	Engaged users' cognitive effort during login	Performance data, effectiveness	Visual paths enhance secure, thoughtful login
Curran et al. [47]	Weak password choices post-training	Cognitive load theory in training	Improved password creation behavior	Post-training password quality	Cognitive training boosts password strength

4.3. Cognitive Password for Password Fatigue

This section reviews current research on cognitive passwords as a response to password fatigue, a condition caused by the mental strain of managing multiple credentials. The authors [6] presented the Cognitive passwords as a promising approach by leveraging personal knowledge and experiences to enhance memorability and security, which is performed through interactive question-answer dialogues based on personal facts. These systems improve recall and resist guessing even from individuals close to the user. Moreover, usability is further enhanced by adaptive frameworks like UCAPP, which tailor password complexity to individual cognitive capacities, assessed using tools such as the Cognitive Burden Scale (CBS). Addressing cognitive fatigue is essential, as prolonged mental effort can increase errors and security risks. Studies have explored AI-based tools like DeepPasswd, revealing how security fatigue, user traits, and workload affect engagement [48]. Findings show that younger users are less likely to engage with the tool, and individual differences such as anxiety and trust influence its use. Similarly, cognitive OTP systems reduce fatigue by sending authentication questions through third-party platforms, reducing the memory burden [37]. Personalized cognitive schemes using familiar images or CAPTCHA-style reminders have also shown promise in improving recall and reducing weak password reuse [35]. Other systems monitor login attempts and offer cognitive aids after repeated failures, improving usability and minimizing frustration [40]. Despite their advantages, some cognitive methods, particularly those involving complex, recall may contribute to fatigue and lead users to unsafe practices such as reusing passwords or sharing credentials [49]. Therefore, while cognitive passwords help mitigate fatigue, further research is required to tailor solutions to diverse user needs. A summary of relevant research on password fatigue and cognitive authentication is provided in **Table 3**.

Table 3. The summary of the existing works in cognitive password for Fatigue.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Krzyworzeka et al. [35]	Fatigue from password reuse or forgetfulness	Personalized image-based CAPTCHA reminders	Links passwords to personal images for easier recall	Image association data	Improves recall and discourages reuse of weak passwords
Deluca et al. [40]	Strain from remembering complex passwords	Prompting cognitive aid after failed login attempts	Offers assistance to reduce mental effort post-failure	Login monitoring	Enhances usability by reducing stress during login failures

Table 3. *Cont.*

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Matthews et al. [48]	Security fatigue and variation in user tool engagement	AI-powered password generator (DeepPasswd)	Examines user differences and fatigue in using AI tools	Task performance, user traits (anxiety, trust, etc.)	User traits affect tool usage; younger users engage less with password tools
Zviran et al. [16]	Managing many passwords	Cognitive OTP system with third-party questions	Increases security and reduces memory load	Cognitive OTP generation	Supports secure access while reducing memory strain from multiple passwords
Zviran et al. [50]	Burden from complex password requirements	Informal methods (e.g., sharing credentials, storing files)	Reveals coping behaviors in response to password complexity	User behavior observations	Users adopt ad-hoc strategies to manage cognitive burden and maintain access
Al-Slais et al. [6]	Cognitive burden from managing multiple passwords	Cognitive password methods based on personal knowledge and experience	Enhances memorability and security through user-tailored passwords	UCAPP, Cognitive Burden Scale (CBS)	Cognitive passwords reduce fatigue by aligning with individual cognitive limits

4.4. Cognitive Passwords for Scalability and Adoption

Cognitive passwords present a promising authentication mechanism that supports both scalability and wide adoption across diverse user environments. Their design leverages personal knowledge, opinions, and contextual cues, enabling users to recall credentials more easily while preserving high security standards [50]. Since the answers are inherently tied to the user, these methods are resistant to guessing even by individuals who personally know the user, providing an advantage over traditional password schemes [50,51]. Scalability is achieved through several design features and implementation models. Adaptive cognitive prompts that adjust based on a user's login history help streamline authentication in large systems with repeated access attempts [40], while cognitive one-time passwords (OTPs) delivered through third-party platforms eliminate the need for storing static secrets and thereby reduce management overhead [37]. Additional scalable models include story-based passwords that encode memorable narratives with high entropy [27], Visual CAPTCHA-based cognitive challenges tailored to domain-specific knowledge [52], and recovery models that infer password-creation logic to reduce brute-force dependency in forensic investigations [53,54]. These characteristics not only enhance scalability but also improve system adoptability. Cognitive password approaches align well with user preferences across diverse and high-density environments by offering adaptable, user-centered interaction flows [51]. However, reliance on personal information introduces privacy concerns, reinforcing the need for strong data-protection practices and carefully designed system governance. **Table 4** presents an integrated summary of the key studies addressing scalability and adoption in cognitive password research.

Table 4. Summary of Existing Work on Cognitive Passwords for Scalability and Adoption.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Grunin et al. [37]	Limitations of traditional password storage	Cognitive OTPs distributed via third-party systems	Removes dependence on static password storage	OTP generation and delivery testing	Enhances scalability and supports broader adoption through reduced storage requirements
Deluca et al. [40]	Managing repeated login attempts in large systems	Adaptive prompts based on login-attempt history	Improves user flow and reduces login friction	Monitoring of login behaviors	Cognitive prompts facilitate scalable and user-friendly authentication, improving adoptability
Doerr et al. [51]	Need for memorable yet secure credentials	Personal facts and opinion-based cognitive inputs	Provides high memorability and resilience to guessing	User recall and density analysis	Cognitive password designs scale well across diverse populations and support adoption
Werner et al. [27]	Weaknesses in traditional password security for distributed platforms	Text-based story or narrative passwords	Balances memorability with strong entropy	Story structure and composition analysis	Story-driven authentication improves scalability and system acceptance
Ogiela et al. [52]	Scalability in expert-driven or specialized environments	Visual CAPTCHA-based cognitive challenges	Enables trusted authentication requiring domain expertise	Expert validation studies	Suited for scalable deployment in contexts requiring specialized cognitive checks

Table 4. *Cont.*

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Fragkos et al. [53]	Low entropy in traditional passwords	Textual story-based cognitive password model	Increases entropy while maintaining recall	Narrative analysis and usability testing	Story-based methods provide secure and scalable authentication options
Alrubaish et al. [54]	Inefficient brute-force-driven password recovery	Logic-based cognitive password recovery frameworks	Enables faster and more efficient recovery processes	Forensic recovery simulations	Enhances scalability in digital forensics and supports system-wide adoption

4.5. Cognitive Passwords for Authentication

This section discusses cognitive password authentication, which leverages user cognition, memory, and emotional engagement to improve both security and usability. Cognitive password methods encompass graphical passwords, cognitive biometrics, and context-aware systems. Graphical Passwords replace traditional alphanumeric input with user-selected images or sequences, enhancing memorability and reducing password reuse [33]. Cognitive Biometrics, such as ECG and EEG signals, offer unique, universal identifiers resistant to spoofing; however, they require further development for mainstream deployment [54]. Emotionally Engaged Neurosymbolic AI (EENAI) generates passwords using emotional context, enhancing both recall and security [55]. Context-Aware Models, like the use of Google Street View images tied to personal experiences, embed password reminders into the login process to support strong and memorable credentials [39]. Despite their promise, cognitive password systems may face adoption challenges, including infrastructure requirements and user acceptance. Several studies reinforce the benefits of cognitive-based approaches. For instance, cognitive development influences children's password behaviors, suggesting the need for age-specific cybersecurity education [19]. Hybrid models using ambiguous illusion images as graphical passwords also improve usability and resistance to attack [56]. EEG-based authentication reduces memorization effort while offering strong biometric protection [15]. Additionally, CAPTCHA-like challenges embedded with AI-hardness characteristics aim to secure client-server communication without revealing password data [57]. Other contributions include systems based on cognitive CAPTCHA codes, which require specific domain knowledge for authentication, particularly useful in secure, distributed environments [52,58]. Hybrid models combining cognitive biometrics and user profiling have also been proposed to improve personalization and system adaptability [59]. Lastly, keystroke dynamics offer a cognitive-behavioral approach for both user verification and identification [44]. Collectively, these cognitive techniques aim to strengthen authentication by aligning with users' cognitive capacities, reducing the burden of memorization while maintaining security [60]. A summary of the key studies on cognitive passwords for authentication is presented in **Table 5**.

Table 5. The Summary of the Existing Works in Cognitive Password for Authentication.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Sodhro et al. [15]	High memorization load	EEG-based biometrics	No need to remember passwords	EEG readings	Increases security and reduces cognitive load
Patil et al. [33]	Users forget passwords easily	Graphical passwords (image/sequence)	Improves recall and reduces reuse	Image/sequence selection	Easier to remember and more secure than text passwords
Kävrestad et al. [19]	Weak habits in children	Cognitive analysis (memory/problem-solving)	Highlights education needs for stronger passwords	Cognitive skills	Education should align with cognitive ability
Krzyworzeka et al. [39]	Hard to create memorable long passwords	Google Street View images	Uses personal visual memory for stronger passwords	Personal experience	Personal cues improve recall and strength
Khare et al. [44]	Unreliable user verification	Keystroke dynamics	Identifies users via typing patterns	Typing behavior	Effective for ID and verification
Werner et al. [27]	Weak cloud password security	Visual CAPTCHA + cognitive codes	Enhances trusted access via expertise	Expertise-based input	Strengthens access with cognitive + visual checks
Biswal	Spoofing in traditional methods	Cognitive biometrics (ECG, EEG)	Spoof-resistant authentication	ECG/EEG signals	Secure but needs more development
Dabeer et al. [56]	Poor password memorability	EENAI system	Generates emotionally-linked secure passwords	Emotional context	Balances security and recall
Raghavasimhan et al. [57]	Passwords are often forgotten	Ambiguous illusion images	Boosts recall and security using image tags	Blurred image with tags	Better than text passwords

Table 5. *Cont.*

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Ogiela et al. [58]	Slow authentication	NLP with text-based input	Uses language analysis for faster login	NLP response analysis	Enhances speed and cognitive fit
Awad et al. [59]	Insecure authentication	Multi-stage cognitive CAPTCHA	Requires problem-solving for access	CAPTCHA success rates	More secure via cognitive challenge
Belk et al. [60]	Client-server password risks	AI-hard CAPTCHA challenges	Secures login without sending passwords	CAPTCHA strength	Improves security but focused on cognition
Perini [61]	No user personalization	Hybrid cognitive biometrics	Adapts authentication to the user	Biometric profiling	Personalization improves usability and security

4.6. Cognitive Password for Accessibility

Cognitive passwords offer an innovative approach to enhancing accessibility in authentication systems, particularly for individuals with cognitive disabilities. By leveraging users' cognitive processes, these systems simplify the login experience, making it more intuitive and less mentally demanding. Design principles that support cognitive accessibility include minimalist interfaces, which reduce cognitive load by limiting the number of elements presented to the user [61], as well as development guidelines to help IT professionals create authentication systems tailored to diverse cognitive abilities [62]. Cognitive biometric systems such as ACSSECR utilize unconscious responses to stimuli, allowing users to authenticate by recognizing a "Cogkey" without complex enrollment, procedures thus improving accessibility [61]. Similarly, cognitive password entry systems monitor login attempts and provide cognitive aid prompts to assist users who struggle with traditional logins, easing access to digital resources [40]. Despite these advantages, ensuring usability across all user groups remains a challenge. Research has shown that users with cognitive impairments often struggle with remembering usernames and passwords, keyboard use, logging out, and recognizing login errors, highlighting the need for more accessible systems [63]. While some studies do not specifically address cognitive passwords, they emphasize the importance of simplicity and relevant information presentation in improving digital accessibility [63]. Other works propose picture-based cognitive authentication, which supports memory recall through image recognition rather than textual input, offering a secure and user-friendly alternative [28]. In the context of inclusive design, studies also stress the importance of creating digital environments, especially in e-Learning, that accommodate users with cognitive disabilities [64]. Cognitive passwords improve accessibility by incorporating personal facts and opinions that are easier to remember, thereby reducing cognitive load and improving usability [50]. Narrative-based password systems further enhance accessibility by using visual or auditory formats suited for users with sensory impairments or limited literacy [43]. Some models even assess users' cognitive ability through testing, restricting access when thresholds are not met, and an approach that doubles as a security and safety mechanism [65]. Additionally, graphical password models aligned with ISO usability standards have demonstrated positive feedback in terms of accessibility and overall user satisfaction [31]. As cognitive password systems evolve, they must maintain a balance between being accessible for users with cognitive challenges and usable for the general population. **Table 6** summarizes the key contributions to accessibility in cognitive password research.

Table 6. The Summary of the Existing Works in Cognitive Password for Accessibility.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Sarkhoshi et al. [31]	Graphical password accessibility concerns	Graphical model with ISO usability standards	Assesses usability of graphical passwords	User feedback data	Confirms accessibility and usability of graphical schemes
Deluca et al. [40]	Difficulty remembering and typing passwords	Cognitive password entry with prompts	Offers memory assistance during login	Prompted login attempts	Reduces login errors through cognitive support
Hoover et al. [43]	Difficult for impaired users to use traditional passwords	Visual/auditory narrative passwords	Enhances access for sensory/literacy-impaired users	User interaction data	Narrative formats improve accessibility significantly
Goldberg et al. [20]	Standard authentication lacks accessibility	Keyboard layout, character mapping, pattern recognition	Focused on password strength but neglected accessibility	Keyboard/pattern input	Fails to address accessibility needs in cognitive authentication

Table 6. *Cont.*

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Doerr et al. [51]	Mental load of password recall	Personal fact-based cognitive passwords	Lowers memory effort while boosting usability	Recall of personal information	Personal data-based passwords improve accessibility
Di Campi et al. [62]	High cognitive demand in authentication	Cognitive biometric systems (ACSSECR, Cogkey)	Enables easy login with minimal training via stimulus recognition	User recognition of Cogkey	Improves accessibility with low effort and high usability
Hayes et al. [63]	Limited support for users with disabilities	Biometric authentication	Highlights importance of inclusivity in design	Biometric usage data	Biometrics enhance accessibility for disabled users
Weinshall [28]	Inaccessible web authentication interfaces	Clear design and simple principles	Promotes user-friendly design standards	Web accessibility metrics	Encourages streamlined, accessible web authentication
Weinshall [28]	No cognitive testing in authentication	Cognitive identification devices	Uses tests to validate user access securely	Cognitive test scores	Testing enhances both security and accessibility
Dirks et al. [64]	Password recall issues	Picture-based cognitive authentication	Offers secure, easy-to-remember alternatives	Picture recognition success	Aids memory-challenged users with accessible login options
Kukawka et al. [65]	Inaccessibility in digital systems	Accessible eLearning design	Encourages inclusive design for cognitive limitations	User engagement metrics	Promotes cognitively inclusive digital environments
Borina et al. [66]	Cognitive impairments hinder authentication	Supportive authentication systems	Reveals issues in interface and password handling	User performance results	Emphasizes need for accessible systems for cognitively impaired users
Woods et al. [67]	Need to ensure cognitive accessibility	Cognitive function evaluation tools	Validates user capability before access	Cognitive test evaluations	Enhances system design by verifying cognitive readiness

4.7. Cognitive Passwords for Understanding Humans Memory and Cognition

Traditional password systems often suffer from poor memorability and weak security due to the limitations of human memory and predictable user behavior. In response, cognitive passwords have emerged as an innovative solution that leverages human memory, perception, and cognitive processes to enhance both security and usability. Unlike conventional passwords, cognitive passwords are based on personal facts, preferences, or experiences, making them easier to recall while remaining difficult for others to guess [50]. These systems typically involve users engaging in dynamic dialogues, responding to rotating questions tied to their personal history, which enhances both memorability and resistance to attacks. Incorporating theories of memory, such as working memory and long-term memory principles, has enabled researchers to develop more secure and user-centric authentication practices. For example, cognitive signatures like visual search behavior and memory-based tasks have been explored as robust alternatives to textual passwords [68]. Visual cues, such as images used in password creation, have been shown to increase entropy without compromising ease of recall. Moreover, systems like PassShapes allow users to generate passwords through geometric strokes, further reducing cognitive burden [4]. Cognitive assessments may also help ensure that only users with sufficient mental capacity can access sensitive systems. However, despite these advancements, privacy concerns and the risk of cognitive overload remain critical challenges that must be addressed to ensure broad user adoption. Several studies have contributed to the development of cognitive password systems. The use of memory techniques like list reduction has been shown to enhance multiple-password recall by minimizing interference, aligning with long-term memory theory [12]. WPRTP, a graphical password approach based on drawing patterns on a grid, demonstrated improved memorability and faster login times compared to traditional alphanumeric methods [69]. Additionally, research has found that personalization improves recall but does not necessarily enhance secrecy, indicating the need for stricter password guidelines [14]. Other studies suggest that users underestimate their memory capabilities, with perceived memory limitations, not actual memory deficits, being a significant barrier to secure password practices [67]. Comparisons between graphical and text-based passwords have shown that the former produce fewer short-term memory errors and are less prone to interference [70]. Novel approaches, such as imprinting behaviors, and non-transferable memory traits, have also been explored as unique cognitive identifiers in secure authentication systems [71]. Furthermore, EEG-based cognitive signatures and behavioral biometrics like keystroke dynamics have demonstrated promise for secure, user-friendly identification [44]. Cognitive codes that integrate emotional or experiential memory, such as those used in story-based or visual recognition schemes, further enhance password recall without compromising security [43]. In summary, cognitive passwords offer a promising direction in authentication research by aligning with users' natural cognitive strengths. They reduce reliance on memory-intensive tasks, enhance user compliance, and increase security. Nonetheless, continued research is essential to address issues of scalability, privacy, and cognitive overload. **Table 7** provides a summary of the research on cognitive passwords in challenges for Understanding Human Memory and Cognition.

Table 7. Summary of Existing Works in Cognitive password for Understanding Human Memory and Cognition.

Ref.	Problem	Techniques Used	Contributions	Measurements	Conclusion
Woods [13]	Difficulty recalling multiple passwords	List reduction method using long-term memory principles	Reduces interference, improving password recall	Recall performance metrics	Enhanced recall by minimizing cognitive interference
Lazar et al. [14]	Insecure password behavior from poor memory	Cognitive signatures and memory insights	Improves understanding to reduce insecure password practices	Cognitive signature analysis	Memory insights enhance security and reduce poor behaviors
Horcher et al. [41]	Weak secrecy in personalized passwords	Personalization of cognitive passwords	Improves recall but not secrecy; stricter security needed	Recall and secrecy metrics	Personalization aids recall but fails to enhance secrecy
Weiss et al. [4]	Difficulty memorizing passwords	PassShapes: stroke-based input passwords	Enhances memorability and reduces cognitive load	Recall and cognitive load	Stroke-based input improves memorability and lowers load
Khare et al. [44]	Secure user identification challenges	Imprinting behaviors as identity certificates	Novel use of unique behaviors for secure ID	Behavioral imprint analysis	Imprinting behaviors provide secure, unique identification
Doerr et al. [51]	Difficulty recalling traditional passwords	Cognitive passwords using personal facts/experiences	Enhances security and recall with personalized, rotating questions	User recall performance	Cognitive passwords improve memorability and security
Chiasson et al. [70]	Interference between recall methods	Comparison of text vs. graphical passwords	Graphical passwords resist interference better in short term	Recall performance	Graphical passwords easier short-term recall, similar long-term
Weinshall [71]	Leveraging human memory for security	Imprinting behaviors for authentication	Uses unique behaviors as non-transferable identity certificates	Memory behavior analysis	Imprinting behaviors have potential for secure authentication
Camp et al. [72]	Few alternatives to traditional passwords	Cognitive signatures via visual search and working memory	Offers robust, unique alternative authentication	Uniqueness of cognitive signatures	Effective and secure alternative authentication method
Li et al. [73]	Password memorability vs. security	Cognitive, word association, conventional passwords	High recall but also high guess rates for cognitive passwords	Recall and guessing rates	Cognitive passwords recall well but need better security
Shuart et al. [74]	Balancing password memorability and entropy	Image-based password generation and recall	Raises entropy while maintaining memorability	Password entropy and recall	Image passwords improve both security entropy and recall
Woods et al. [75]	Low memorability of passwords	Repetition during password creation	Multiple verifications during creation boost memorability	Verification and recall rates	Repetition significantly improves password memorability
Lamond et al. [8]	Memory limits recalling multiple passwords	Metamemory theory applied to password context	User perception of memory limits is main barrier	Recall rates, metamemory analysis	Users recall more than they believe; perception is key factor

5. Cognitive Passwords with Cybersecurity

Cognitive security incorporates cognitive computing principles into cybersecurity strategies, particularly for enhancing user authentication and mitigating risks such as identity spoofing or social engineering attacks. Rather than supplanting human decision-making, the goal of cognitive security is to augment it. In this context, cognitive passwords offer a novel solution by applying cognitive science to design authentication systems that are both secure and user-friendly, overcoming the limitations of traditional passwords. Various approaches have been explored, including Cognitive OTP, which presents users with context-specific questions delivered through third-party platforms. This approach enhances security by making the authentication process context-aware and less predictable [37]. Augmented cognition techniques have also been employed to improve password memorability by modifying character properties, thereby reducing the cognitive load and discouraging insecure practices such as writing down passwords [38]. Another innovative method is the use of narrative passwords, where password elements are embedded within short stories. This technique leverages narrative memory to enhance recall and durability over time [43]. Several studies have contributed to expanding cognitive password applications in cybersecurity. For instance, accessible cognitive password systems benefit from minimalist design principles, reducing cognitive demands and aiding users with cognitive disabilities [62]. Research also demonstrates the cost-effectiveness of opinion-based cognitive passwords, which improve recall and resist guessing while requiring minimal additional resources [5]. Techniques derived from cognitive psychology, such as the method of loci and link method, have been used to strengthen the memorability of system-generated passwords, effectively addressing the classic usability-security trade-off [76]. Behavioral and cognitive biometrics, when integrated with cognitive passwords, bolster defenses against shoulder-surfing attacks while improving usability and recall [44]. Moreover, cognitive cryptography introduces personalized cryptographic protocols, enhancing data security in cloud environments through the use of user-specific cognitive patterns [77]. Additional contributions include the use of pattern recognition algorithms that map user input to keyboard layouts to enforce the creation of strong, unique passwords [20], as well as contextual mnemonic phrase passwords, which employ contextual cues to boost both strength and memorability [78]. Furthermore, dynamic persuasive strategies, though not inherently cognitive, utilize psychological models to nudge users toward creating stronger, more secure passwords [79]. Collectively, these methods illustrate the broad applicability and benefits of cognitive password systems, particularly in improving cybersecurity without sacrificing user experience. In summary, cognitive password mechanisms such as narrative and one-time cognitive passwords represent a significant advancement in securing authentication processes. By incorporating cognitive science principles, these systems yield passwords that are not only more secure and resilient against attacks but also easier to remember and harder to share. Nonetheless, challenges persist in promoting user adoption and achieving a balance between security and usability. As research in this field evolves, continued refinement and user-centered design will be key to fully realizing the potential of cognitive passwords in cybersecurity. **Table 8** summarizes existing works in Cognitive Passwords with Cybersecurity.

Table 8. The Summary of the Existing Works in Cognitive Passwords with Cybersecurity.

Ref.	Techniques	Description	Contributions	Benefits	Challenges
Haga et al. [3]	Cost-effective Security	Integrating cognitive items with traditional passwords.	Cognitive items improve recall and enhance security without significant investment.	Low-cost solution for improved security.	Integration with traditional systems can be complex.
Grunin et al. [37]	Cognitive One-Time Passwords (OTP)	Contextually relevant questions for OTP generation.	Third-party platforms deliver questions for enhanced security.	More secure OTPs by preventing guessability.	Relies on third-party platforms, privacy concerns.
Mogire et al. [38]	Augmented Cognition in Passwords	Improving password recall through cognitive techniques.	Transforms character properties to make passwords easier to remember.	Reduces cognitive load and minimizes insecure practices.	May require user adaptation to new methods.
Hoover et al. [43]	Narrative Passwords	Short stories used to create memorable passwords.	Binds password elements in a narrative to enhance memory.	More memorable passwords, harder to forget.	Potential for over-simplification of stories leading to weak passwords.
Khare et al. [44]	Behavioral and Cognitive Biometrics	Combining cognitive passwords with behavioral biometrics.	Prevents shoulder-surfing and improves security by combining biometrics with passwords.	Improved security and ease of recall.	Privacy concerns with biometric data collection.
Goldberg et al. [20]	Pattern Recognition for Stronger Passwords	Mapping user-entered passwords to keyboard layouts.	Applies pattern recognition algorithms to create stronger, unrepeatable passwords.	Stronger, unique passwords that enhance cybersecurity.	Risk of pattern recognition algorithms being bypassed.
Hayes et al. [63]	Cognitive Passwords for Accessibility	Minimalist design for reducing cognitive demands in training.	Applies minimalist design to accessible password systems.	Easier to use for individuals with cognitive disabilities.	Balancing security with accessibility can be difficult.
Haque et al. [76]	Memory Enhancement with Cognitive Psychology	Techniques like the method of loci and the link method to improve recall.	Enhances user recall and password security, addressing the usability-security trade-off.	Better memorability and security of system-assigned passwords.	Memory techniques may be unfamiliar to users.
Ogiela et al. [77]	Cognitive Cryptography	Personalized cryptographic protocols for password management.	Enhances data security and password management in cloud environments.	Better cybersecurity and password management.	Complexity in implementation for cloud environments.
McEvoy et al. [78]	Contextualizing Mnemonic Phrase Passwords	Use of contextual cues to enhance mnemonic passwords.	Enhances password strength and memorability by leveraging context.	Stronger and more memorable passwords.	Context cues must be carefully chosen to avoid overuse.
Lahza et al. [79]	Dynamic Persuasive Strategies	Encouraging users to create stronger passwords using psychological models.	Can improve password security by persuading users to choose more secure passwords.	Encourages better user practices.	Users may resist persuasive strategies.

Cognitive passwords, by leveraging cognitive psychology, have emerged as a significant advancement in enhancing cybersecurity, making password systems more secure, memorable, and user-friendly.

6. Cognitive Passwords with AI

Cognitive password systems integrated with AI offer transformative improvements in both security and usability for authentication mechanisms. These systems utilize AI to generate passwords that are not only robust but also tailored to individual users, enhancing memorability through emotional engagement and personalized information. One notable approach is the Emotionally Engaged Neurosymbolic AI (EENAI) system, which incorporates emotional valence and arousal to create context-aware passwords that are both secure and easy to recall. Evaluations of EENAI have demonstrated high password strength while maintaining usability [55]. The concept of Cognitive OTP adds another layer of protection by requiring users to answer dynamically generated, context-relevant questions. This technique enhances both cognitive engagement and resistance to unauthorized access [37]. Similarly, graphical password systems, such as the Password Authentication using AI (PAAI), convert textual passwords into visual representations. By leveraging users' visual memory, these AI-generated images improve memorability without compromising security [80]. Moreover, the researchers [81] explored the password security through a two-phase approach: a user survey revealing gaps between awareness and practice, and an ML analysis of leaked passwords showing that password length is the key factor influencing strength classification. Despite the significant advantages offered by AI-enhanced cognitive passwords, including improved password strength, personalization, and user engagement, challenges remain. Key concerns include maintaining user trust, ensuring consistent usability across diverse populations, and mitigating risks such as social engineering. As the field advances, achieving an optimal balance between security, user experience, and cognitive load will be critical. **Table 9** summarizes the existing research and implementations in cognitive password augmented with AI.

Table 9. The Summary of the Existing Works in Cognitive Passwords with AI.

Ref.	Technique	Description	Contributions/Studies	Benefits	Challenges
Biswal [55]	Emotionally Engaged Password Generation	EENAI generates context-aware passwords based on emotional valence and arousal.	Balances security and usability while enhancing memorability.	Stronger, memorable passwords through emotional engagement.	Concerns about user emotional privacy and data security.
Grunin et al. [37]	Cognitive One-Time Passwords (OTP)	Sends contextually relevant questions for users to answer for access.	Adds cognitive engagement during authentication, making it harder to guess.	Adds another layer of security, harder to bypass.	Dependency on real-time question generation, privacy concerns.
Huang et al. [80]	Graphical Passwords	AI generates images from textual passwords for easier recall.	Combines visual memory with AI to create secure and user-friendly passwords.	Enhances memorability by leveraging visual memory.	Potential for graphical password systems to be bypassed or misused.

7. Existing Solutions and Techniques for Cognitive Passwords

Various solutions and techniques have been developed to address the challenges associated with cognitive passwords, focusing on improving memorability, security, and usability. Below is an overview of these existing techniques. **Table 10** presents the existing solutions and techniques for cognitive passwords.

Table 10. The summary for the section on Existing Solutions and Techniques for Cognitive Passwords.

Ref.	Limitations& Challenges	Solutions	Technique Name	Brief Description
Dias et al. [1]	Password Memorability	Use cognitive passwords with personal information	Cognitive Passwords	Utilize personal information (e.g., names, dates, places) to create memorable passwords.
Palmgren et al. [2]	Password Guessing Resistance	Implement cognitive password techniques like story-based passwords	Story-Based Passwords	Users create passwords based on personal stories, which makes them more resistant to guessing attacks.
Haga et al. [3]	Password Usability	Introduce cognitive password techniques, such as image-based passwords	Image-Based Passwords	Users select images to create passwords, improving usability and memorability.
Li et al. [73]	Password Security	Employ cognitive password techniques like cognitive biometrics	Cognitive Biometrics	Measures cognitive behaviors (e.g., reaction time, accuracy) to enhance password security.
Campbell et al. [82]	Password Management	Implement cognitive password techniques like password vaults with cognitive authentication	Cognitive Authentication	Utilizes cognitive techniques, such as facial or voice recognition, to authenticate users and manage passwords.

There are several key techniques in cognitive password systems designed to improve both security and usability. Cognitive passwords utilize personal information such as names, dates, and places to create passwords that are more memorable by being personally relevant, thus addressing the complexity issues of traditional passwords. Story-based passwords encourage users to base their passwords on personal narratives or experiences, which enhances memorability and makes them harder to guess, adding complexity against attackers. Image-based passwords allow users to select pictures instead of text, leveraging visual memory to improve recall and ease of use compared to conventional alphanumeric passwords. Another promising technique is cognitive biometrics, which strengthens security by analyzing users' cognitive behaviors during authentication (such as reaction times and accuracy), adding a behavioral layer that helps prevent unauthorized access through impersonation or social engineering. Finally, cognitive authentication methods, including facial recognition and voice authentication, enable users to authenticate based on unique cognitive and biometric traits, reducing reliance on remembered complex passwords and increasing both convenience and security. In summary, cognitive passwords, especially when enhanced by AI, offer a compelling solution to the enduring challenges of password security and user-friendliness. AI-powered methods such as emotionally engaged password generation, deep learning–based user-centric password creation, and cognitive biometrics substantially improve password strength and memorability. Nonetheless, ensuring strong protection against social engineering and phishing attacks while maintaining user engagement remains a critical challenge. These innovations are shaping the future of cybersecurity by enabling authentication systems that are more secure, personalized, and accessible.

8. Cognitive Password System

This research evaluates the performance of cognitive password authentication systems as an alternative to conventional password methods. The results demonstrate that cognitive passwords bolster security by utilizing individuals' personal memories, behaviors, and contextual understanding, thereby increasing resistance against phishing, social engineering, and brute-force attacks. Moreover, these systems enhance usability by lowering the chances of password fatigue and forgotten credentials, as users rely on familiar information instead of random character sequences. However, challenges to broader adoption remain, including privacy concerns, difficulties in designing effective cognitive prompts, and vulnerability to social engineering tactics. The incorporation of AI and machine learning (ML) has further advanced these systems by enabling personalized and adaptive authentication, which improves both security and user experience. Additionally, cognitive authentication methods contribute to accessibility, benefiting users with disabilities. Various techniques such as graphical passwords, emotion-aware mechanisms, and narrative-based prompts exhibit differing success in balancing usability, memorability, and security. Nonetheless, achieving this balance is a design challenge, particularly when aiming to minimize cognitive burden while preventing guessability. The cognitive system is illustrated in **Figure 4**.

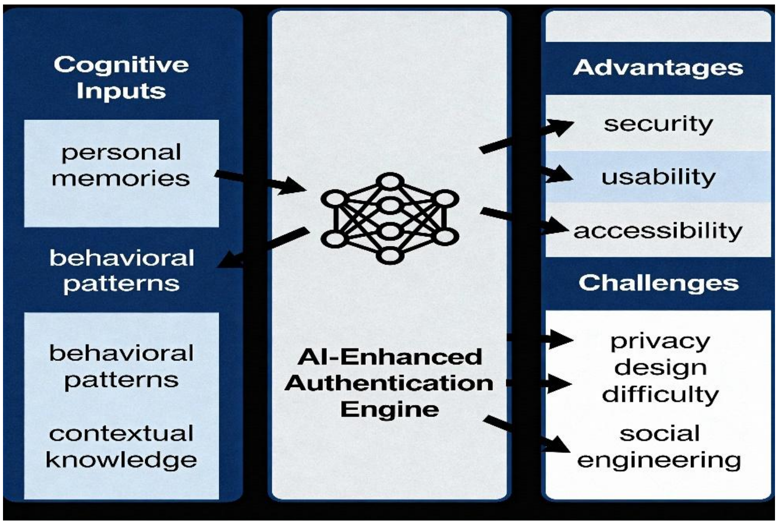

Figure 4. Cognitive Password System.

Moreover, **Table 11** shows a summary of the principal cognitive design strategies assessed in this study.

Table 11. Design Techniques in Cognitive Password Systems.

Design Solution	Techniques Used	Brief Description
Graphical Passwords	Visual cues, image-based methods	Enhance memorability through visual input, but face security and scalability concerns.
Cognitive Biometrics	Behavioral traits, unique user patterns	Improve security via behavioral profiling, though require complex data collection.
Emotion-Aware Passwords	Emotion detection, adaptive interactions	Adjust to users' emotional states, lowering mental load but raising privacy issues.
Cognitive One-Time Passwords	Context-aware, personalized challenges	Generate dynamic, harder-to-guess passwords based on individual context.
Narrative-Based Passwords	Storytelling, memory associations	Improve recall by embedding authentication in personal stories or experiences.
Cognitive CAPTCHAs	User interaction, logic-based problem solving	Authenticate through cognitive tasks rather than memorized inputs.
Personalized Models	AI and user profiling	Tailor authentication to user profiles for better security-usability balance.

In brief, this study highlights cognitive password systems as a promising alternative to traditional passwords by leveraging users' personal memories and behaviors to improve security and usability. Integration of AI and ML enhances personalization and adaptability, while accessibility benefits users with disabilities. However, challenges like privacy issues and social engineering risks remain, and balancing memorability with security continues to be a key design challenge. Based on the above discussion, an enhanced framework of the cognitive password system is proposed, as shown in **Figure 5**.

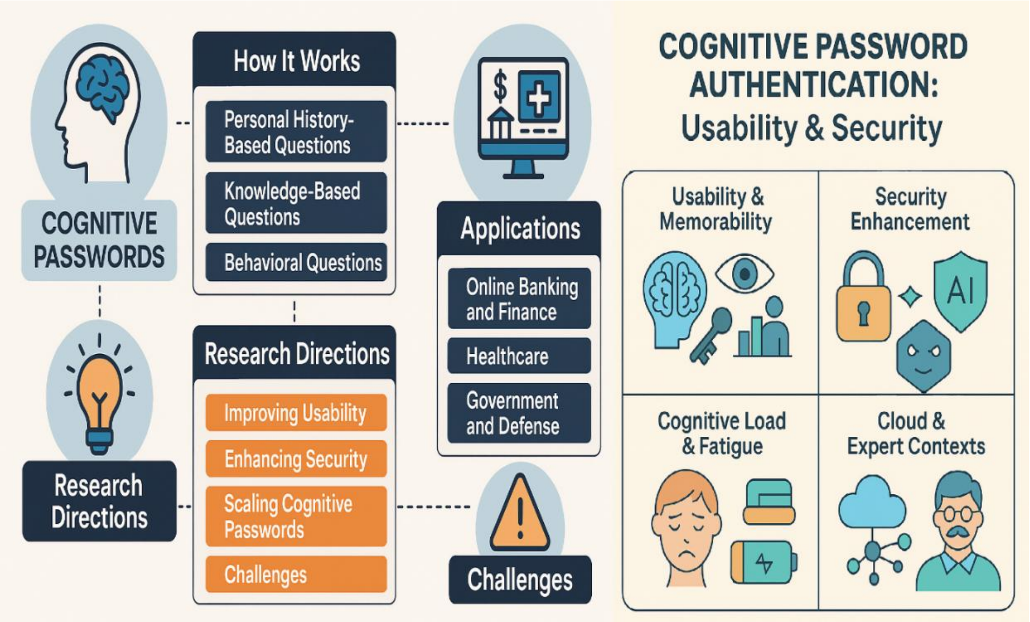

Figure 5. Enhanced framework of the cognitive password system.

9. Discussion

This study highlights that cognitive password systems offer significant advancements over traditional authentication methods by improving both security and usability. By leveraging users' memories, experiences, and cognitive behaviors, these systems provide more personalized, intuitive, and memorable authentication processes. Methods such as graphical passwords, narrative-based approaches, and cognitive OTPs apply cognitive psychology principles to resist common attacks, including phishing, shoulder surfing, and password reuse, while enhancing memorability and user experience. Despite their potential, several limitations constrain widespread adoption. Usability challenges are particularly pronounced for individuals with cognitive impairments, limited technical literacy, or cultural differences that affect the interpretation of authentication prompts. Cognitive overload, resulting from overly complex or ambiguous tasks, can reduce compliance and satisfaction. Scalability remains a concern, particularly for enterprise or cloud-based deployments, where a large number of users must be supported. Privacy and data protection risks are heightened when AI or ML techniques are employed for adaptive personalization, as sensitive behavioral and emotional data must be carefully managed. Moreover, resistance to social engineering attacks is not yet fully addressed, and the integration of cognitive passwords with multi-factor authentication (MFA), including biometrics, requires a careful balance between security, trust, and user experience. Current research gaps are evident in several areas. There is a lack of systematic empirical evaluation across diverse user populations, environments, and threat models. Standardization of authentication task design and guidelines for seamless integration into existing infrastructures is limited. While AI-enhanced cognitive passwords show promise for personalization and adaptive security, privacy-preserving strategies, ethical data handling, and transparency remain underexplored. Addressing these gaps will be essential to improve usability, strengthen security, and facilitate the broader adoption of cognitive password systems in real-world applications. **Figure 6** illustrates the conceptual framework of this study.

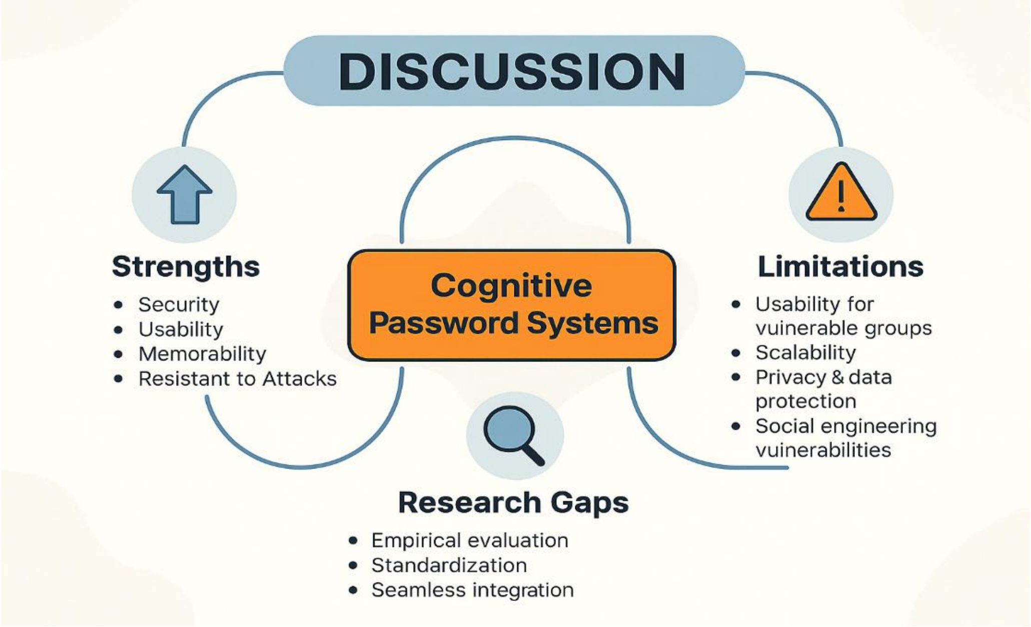

Figure 6. Framework of this Study.

10. Challenges, Limitations, and Future Research Directions

Cognitive password systems have emerged as a promising approach to enhancing authentication security and usability. However, several challenges and limitations persist, which must be addressed to realize their full potential. One key challenge is cognitive overload, where users may experience mental fatigue or confusion due to complex prompts or interaction formats. Future research should focus on designing interfaces and authentication tasks that minimize cognitive load, simplify interactions, and accommodate users with diverse abilities and technical expertise. Another critical concern is user acceptance. Limited familiarity with cognitive password systems and perceived complexity can hinder adoption and long-term viability. Empirical studies, including longitudinal and real-world evaluations, are essential to understand user compliance and guide the development of intuitive, user-centered designs that promote awareness and engagement. Security vulnerabilities, such as susceptibility to phishing, social engineering, or behavioral attacks, remain a significant limitation. Addressing these threats requires robust encryption, multi-factor authentication, and AI-driven anomaly detection, alongside workflow designs that resist manipulation. In parallel, privacy concerns must be carefully managed, as personalized cognitive authentication may expose sensitive information. Integrating privacy-preserving mechanisms, including encryption, anonymization, and transparent consent, is essential to safeguard user data without compromising usability. Scalability poses another challenge. Cognitive password systems must perform reliably across large-scale, heterogeneous environments without degrading usability or security. Future work should focus on frameworks and deployment strategies that enable broad adoption in sectors such as healthcare, finance, and enterprise environments. The integration of cognitive passwords with multi-factor authentication (MFA) and biometrics presents both opportunities and challenges. Combining cognitive methods with behavioral analytics, facial recognition, or voice authentication can enhance security, but careful design is required to maintain usability, trust, and system coherence. Similarly, AI and machine learning integration offers potential for adaptive and personalized authentication. Leveraging AI for context-aware, behavior-driven authentication can improve usability and resilience, provided privacy and ethical considerations are rigorously addressed. In addition, Long-term effectiveness is also critical. Cognitive password systems must remain robust against evolving threats and changes in user behavior. Continuous monitoring, longitudinal studies, and real-world testing are needed to evaluate resilience, durability, and compliance over time. Additionally, a cross-disciplinary approach, combining insights from cybersecurity, cognitive psychology, and human-computer interaction (HCI), can provide a deeper understanding of human cognitive strengths and inform more effective system design. Finally, multi-modal biometric integration represents a promising avenue for enhancing authentication robustness. Combining cognitive passwords with multiple biometric modalities such as facial, voice, and behavioral recognition can improve both security and convenience, creating a comprehensive, user-friendly authentication solution. **Table 12** below summarizes the challenges, open issues, and recommended research directions for cognitive password systems.

Table 12. Summary of challenges, open issues, and Future directions for cognitive password system.

Challenge	Open Issue	Description	Future Directions
Cognitive Overload	Improving Usability	Systems may be mentally taxing or complex.	Simplify tasks, optimize UI, manage cognitive load, and provide intuitive interfaces.
User Acceptance	Long-Term Viability	Limited familiarity may hinder adoption.	Conduct longitudinal studies; promote training and awareness; enhance user experience.
Security Vulnerabilities	Phishing & Social Engineering	Attackers may exploit cognitive knowledge or behavior.	Apply encryption, AI threat detection, MFA, and resilient workflow design.
Privacy Concerns	User Data Protection	Personal information may be exposed during authentication.	Integrate encryption, anonymization, and privacy-preserving AI techniques.
Scalability	Large-Scale Deployment	Systems may struggle in diverse, large-scale environments.	Develop scalable frameworks and test across multiple sectors.
MFA and Biometrics Integration	Seamless Integration	Single-layer authentication may be insufficient.	Integrate with biometrics, behavioral analytics, and MFA for multi-layered security.
AI & ML Integration	Personalized Authentication	Static systems lack adaptability to user behavior.	Leverage AI/ML for dynamic, context-aware, and personalized authentication.
Long-Term Effectiveness	Resilience Over Time	Systems may become vulnerable to evolving threats.	Conduct longitudinal evaluations to ensure durability and compliance.
Cross-Disciplinary Optimization	Cognitive Alignment	Lack of interdisciplinary insights may limit design.	Collaborate across cybersecurity, cognitive psychology, and HCI.
Multi-Modal Biometric Use	Robust Authentication	Cognitive methods alone may be insufficient.	Combine cognitive passwords with facial, voice, and behavioral biometrics.

Addressing these challenges through targeted research and design strategies will facilitate the development of cognitive password systems that balance security, usability, and privacy. Continuous innovation, empirical validation, and interdisciplinary collaboration are essential to ensure these systems are scalable, resilient, and practically viable in real-world applications. **Figure 5** illustrates a conceptual framework linking cognitive mechanisms, identified limitations, and future research directions.

11. Conclusions

Cognitive password systems represent a promising advancement in user authentication, providing enhanced security while improving usability compared to traditional methods. By leveraging cognitive principles, these systems address key limitations of conventional passwords, including memorability, complexity, and vulnerability to common attacks. This study systematically analyzed the evolution, strengths, and challenges of cognitive password models such as graphical passwords, cognitive biometrics, and cognitive OTPs demonstrating that well-designed systems can offer secure, intuitive, and user-centered authentication solutions. The findings highlight the critical role of interdisciplinary integration, particularly the incorporation of insights from cognitive psychology and artificial intelligence, to improve personalization, adaptability, and resilience against attacks. Despite these advantages, significant barriers remain, including social engineering risks, accessibility limitations, cognitive overload, privacy concerns, and scalability challenges for large-scale deployment. Addressing these gaps is essential for practical adoption and wider implementation. Future research should focus on enhancing AI-driven personalization, mitigating cognitive and privacy-related risks, improving scalability, and understanding factors affecting user acceptance. Additionally, strategies to seamlessly integrate cognitive password systems with existing infrastructures will be crucial. Overall, realizing the transformative potential of cognitive passwords requires continued collaboration between researchers, developers, and practitioners to advance secure, user-friendly, and scalable authentication solutions for the evolving cybersecurity landscape.

Author Contributions

M.S.A. provided the main idea for this work, wrote the main manuscript, and designed the figures. M.S.A. is the main author of this paper (Conceptualization, validation, writing original draft preparation); M.M.A.-E.S. provided improvement of the main idea for this work, shared in the writing of the main manuscript, designed the figures, and enhanced the novelty of the paper (Conceptualization, validation, sharing the writing original draft preparation, writing review and editing, and general supervision); M.H.A.-S. acted as the supervisor and provided insights for the paper; M.A.-A. assisted in writing the manuscript and improving its language; G.A.A.A.-M. provided further insights, as well as checked the latest references, and helped with the formatting. All authors have read and agreed to the published version of the manuscript.

Funding

This work received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Not applicable.

Acknowledgments

The authors express their gratitude for the support of the University of Saba Region in proposing this work. Also, the authors further appreciate the anonymous reviewers for their insightful and constructive feedback on earlier drafts.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Dias, N.; Reeja, S. A systematic approach towards enhancing of security and usability of graphical password through cognitive computing and data mining. *Indian J. Comput. Sci. Eng.* **2021**, *12*, 1789–1802. [CrossRef]
2. Palmgren, M.; Byström, M. Cognitive authentication schemes–traditional password replacement? Master Thesis, KTH, School of Computer Science and Communication (CSC), Stockholm, Sweden, 2011.
3. Haga, W.J.; Zviran, M. Question-and-answer passwords: An empirical evaluation. *Inf. Syst.* **1991**, *16*, 335–343. [CrossRef]
4. Weiss, R.D.L.; Alexander, A. PassShapes: Utilizing stroke based authentication to increase password memorability. In Proceedings of the NordiCHI '08: 5th Nordic Conference on Human-Computer Interaction: Building Bridges, Lund Sweden, 20–22 August 2008; pp. 383–392. [CrossRef]

5. Podd, J.B.; Reid, H.J. Cost-effective computer security: Cognitive and associative passwords. In Proceedings of the Sixth Australian Conference on Computer-Human Interaction, Hamilton, New Zealand, 2002; pp. 304–305. [CrossRef]
6. Al-Slais, Y.; El-Medany, W.M. User-centric adaptive password policies to combat password fatigue. *Int. Arab J. Inf. Technol.* **2022**, *19*, 55–62.
7. Gaw, S.; Felten, E.W. Password management strategies for online accounts. In Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 12–14 July 2006; pp. 44–55.
8. Lamond, M.; Wood, L.; Prior, S. Cognitive processes underpinning children's password practice. In Proceedings of the BPS Cyberpsychology Section Annual Conference 2024, Liverpool, UK, 1–2 July 2024.
9. Choong, Y.-Y.; Theofanos, M.; Renaud, K.; et al. *Case Study—Exploring Children's Password Knowledge and Practices*; Workshop on Usable Security (USEC): San Diego, CA, USA, 2019. [CrossRef]
10. Zimmermann, V.; Marky, K.; Renaud, K. Hybrid password meters for more secure passwords–a comprehensive study of password meters including nudges and password information. *Behav. Inf. Technol.* **2023**, *42*, 700–743.
11. Safder, W. Password security, an analysis of authentication methods. Master's Thesis, Luleå University of Technology, Luleå, Sweden, 2024.
12. Zhang, J.; Luo, X.; Akkaladevi, S.; et al. Improving multiple-password recall: An empirical study. *Eur. J. Inf. Syst.* **2009**, *18*, 165–176.
13. Woods, N. Improving the security of multiple passwords through a greater understanding of the human memory. PhD Thesis, University of Jyväskylä, Jyväskylä, Finland, 2016.
14. Lazar, L.; Tikolsky, O.; Glezer, C.; et al. Personalized cognitive passwords: An exploratory assessment. *Inf. Manag. Comput. Secur.* **2011**, *19*, 25–41.
15. Sodhro, A.H.; Sennersten, C.; Ahmad, A. Towards cognitive authentication for smart healthcare applications. *Sensors* **2022**, *22*. [CrossRef]
16. Zviran, M.; Haga, W.J. Cognitive passwords: The key to easy access control. *Comput. Secur.* **1990**, *9*, 723–736.
17. Al-Ameen, M.N.; Wright, M.; Scielzo, S. Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; pp. 2315–2324.
18. Naik, S.R.; Vasudeva, S.S.; Shrilakshmi, K.; et al. Advancements in user security: Enhancing usability with graphical password authentication. In Proceedings of the 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 4–6 January 2024; pp. 454–460.
19. Kävrestad, J.; Hagberg, A.; Roos, R.; et al. Usable privacy and security from the perspective of cognitive abilities. In Proceedings of the 16th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity), Online, 16–20 August 2021; pp. 105–121.
20. Goldberg, I.; McGregor, H.R.; Moore, C.B.; et al. Cognitive password pattern checker to enforce stronger, unrepeatable passwords. U.S. Pat. Appl. US 9836595B1, 23 January 2017.
21. Cabarcos, P.A.; Mayer, P. The more accounts I use, the less I have to think: A longitudinal study on the usability of password managers for novice users. In Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025), Seattle, WA, USA, 11–12 August 2025; pp. 351–369.
22. Loos, L.A.; Ogawa, M.-B.C.; Crosby, M.E. Cognitive variability factors and passphrase selection. In Proceedings of the Augmented Cognition. Human Cognition and Behavior: 14th International Conference, AC 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, 19–24 July 2020; pp. 383–394.
23. Contreras, J. Cognitive cryptography using behavioral features from linguistic-biometric data. *Cryptology ePrint Arch*. **2023**. Available from: https://eprint.iacr.org/2023/046.pdf
24. Alroomi, S.; Li, F. Measuring website password creation policies at scale. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, 26–30 November 2023; pp. 3108–3122.
25. Ogiela, U. Cognitive Cryptography for Data Security in Cloud Computing. *Concurr. Comput. Pract. Exp.* **2020**, *32*. [CrossRef]
26. Kennison, S.M.; Chan-Tin, E. Personality and Cognitive Factors in Password Security Behaviors. *N. Am. J. Psychol.* **2023**, *25*, 599–618.
27. Werner, S.; Hoover, C. Cognitive Approaches to Password Memorability–The Possible Role of Story-Based Passwords. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Boston, MA, USA,

22–26 October 2012; pp. 1243–1247.

28. Weinshall, D. Cognitive Authentication Schemes for Unassisted Humans, Safe against Spyware. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P 2006), Berkeley, CA, USA, 21–24 May 2006; pp. 295–300.
29. Wash, R.; Rader, E. Prioritizing Security over Usability: Strategies for How People Choose Passwords. *J. Cybersecur.* **2021**, *7*, tyab012.
30. Wijayarathna, C.; Arachchilage, N.A. Why Johnny Can't Store Passwords Securely? A Usability Evaluation of Bouncycastle Password Hashing. In Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, Christchurch, New Zealand, 28–29 June 2018; pp. 205–210.
31. Sarkhoshi, M.; Li, Q. Cognitive Graphical Password Based on Recognition with Improved User Functionality. In Proceedings of the 12th CS & IT Conference, Sydney, Australia, 22–24 December 2022; pp. 17–24.
32. Lapin, K.; Šiurkus, M. Balancing Usability and Security of Graphical Passwords. In Proceedings of the Conference on Multimedia, Interaction, Design and Innovation, Warsaw, Poland, 9–10 December 2021; pp. 153–160.
33. Patil, N.; Bhutkar, G.; Patil, P.; et al. Graphical-Based Password Authentication. In Proceedings of the International Conference on ICT for Sustainable Development, Goa, India, 21–23 September 2023; pp. 411–419.
34. Balayogi, G.; Kuppusamy, K.S. An Approach for Mitigating Cognitive Load in Password Management by Integrating QR Codes and Steganography. *Secur. Priv.* **2024**, *7*, e447. [CrossRef]
35. Krzyworzeka, N.; Ogiela, L.; Ogiela, M.R. Cognitive CAPTCHA Password Reminder. *Sensors* **2023**, *23*, 3170.
36. Khan, A.; Chefranov, A.G. A Captcha-Based Graphical Password with Strong Password Space and Usability Study. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–6.
37. Grunin, G.; Nassar, N.M.; Nassar, T.M. System, Method and Computer Program Product for Generating a Cognitive One-Time Password. U.S. Pat. Appl. US 7797336B2, 2 June 1997.
38. Mogire, N.; Ogawa, M.-B.; Minas, R.K.; et al. Forget the Password: Password Memory and Security Applications of Augmented Cognition. In Proceedings of the Augmented Cognition: Users and Contexts: 12th International Conference, AC 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, 15–20 July 2018; pp. 133–142.
39. Krzyworzeka, N.; Ogiela, L.; Ogiela, M.R. Cognitive-Based Authentication Protocol for Distributed Data and Web Technologies. *Sensors* **2021**, *21*, 7265.
40. Deluca, L.S.; Kozloski, J.R.; Mizrachi, B.; et al. Cognitive Password Entry System. U.S. Pat. Appl. US 9942234B2, 30 November 2015.
41. Horcher, A.-M.; Tejay, G.P. Building a Better Password: The Role of Cognitive Load in Information Security Training. In Proceedings of the 2009 IEEE International Conference on Intelligence and Security Informatics, Richardson, TX, USA, 8–11 June 2009; pp. 113–118.
42. Abdrabou, Y.; Abdelrahman, Y.; Khamis, M.; et al. Think Harder! Investigating the Effect of Password Strength on Cognitive Load during Password Creation. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2014; pp. 1–7.
43. Hoover, C.; Werner, S.; Cohen, R. Cognitive Authentication and Narrative Passwords. *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* **2014**, *58*, 1511–1515. [CrossRef]
44. Khare, K.; Rautji, S.; Gaur, D. Behavioural Biometrics and Cognitive Security Authentication Comparison Study. *Adv. Comput.* **2013**, *4*, 15.
45. Ogiela, U.; Ogiela, M.R. Cognitive Approach for Creation of Visual Security Codes. In *Advances in Intelligent Networking and Collaborative Systems. INCoS 2021. Lecture Notes in Networks and Systems*; Barolli, L., Chen, H.C., Miwa, H., Eds.; Springer: Cham, Switzerland, 2022; Vol. 312, pp. 107–111.
46. Greenstadt, R.; Beal, J. Cognitive Security for Personal Devices. In Proceedings of the 1st ACM Workshop on AISec, Alexandria, VA, USA, 27–31 October 2008; pp. 27–30.
47. Curran, K.; Doherty, J.; McCann, A.; et al. Good Practice for Strong Passwords. *EDPACS* **2011**, *44*, 1–13.
48. Matthews, G.; Ateniese, G.; Barbará, D.; et al. Usage of an AI-Based Password Tool: Impacts of Security Fatigue, Age, and Individual Differences. *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* **2024**, *68*, 236–242.
49. Parkin, S.; Krol, K.; Becker, I.; et al. Applying Cognitive Control Modes to Identify Security Fatigue Hotspots. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22 June 2016.
50. Zviran, M.; Haga, W.J. User Authentication by Cognitive Passwords: An Empirical Assessment. In Proceedings of the 5th Jerusalem Conference on Information Technology 'Next Decade in Information Technology',

Washington, DC, USA, 22–25 October 1990; pp. 137–144.

51. Doerr, C.; Colagrosso, M.; Grunwald, D.; et al. Scalability of Cognitive Radio Control Algorithms. In 2008 3rd International Symposium on Wireless Pervasive Computing, Santorini, Greece, 7–9 May 2008; pp. 685–692.
52. Ogiela, M.R.; Ogiela, L. Cognitive Codes for Authentication and Management in Cloud Computing Infrastructures. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2018. Lecture Notes on Data Engineering and Communications Technologies*; Xhafa, F., Leu, F.Y., Ficco, M., et al., Eds.; Springer: Cham, Switzerland, 2019; Vol. 24, pp. 160–166.
53. Fragkos, G.; Tryfonas, T. A Cognitive Model for the Forensic Recovery of End-User Passwords. In Proceedings of the Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), Karlovassi, Greece, 27–28 August 2007; pp. 48–54.
54. Alrubaish, H.; Saqib, N. Your Vital Signs as Your Password? In *Recent Advances in Biometrics*; Sarfraz, M., Ed.; IntechOpen: London, UK, 2022.
55. Biswal, S. Emotionally Engaged Neurosymbolic AI for Usable Password Generation. In Proceedings of the International Conference on Advances in Data-Driven Computing and Intelligent Systems, Pilani, India, 21–23 September 2023; pp. 251–263.
56. Dabeer, S.; Ahmad, M.; Sarosh Umar, M.; et al. A Novel Hybrid User Authentication Scheme Using Cognitive Ambiguous Illusion Images. In *Data Communication and Networks. Advances in Intelligent Systems and Computing*; Jain, L., Tsihrintzis, G., Balas, V., et al., Eds.; Springer: Singapore, 2019; Vol. 1049, pp. 107–118.
57. Raghavasimhan, T.; Manoj, S.; Sweetlin, J.D.; et al. Preventing Cryptographic Attacks Using AI-Hard Password Authentication. In Proceedings of the 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 5–6 April 2023; pp. 1–6.
58. Ogiela, M.R.; Ogiela, L. Authentication Protocols Using Multi-Level Cognitive CAPTCHA. In Proceedings of the Advances in Internet, Data and Web Technologies: the 7th International Conference on Emerging Internet, Data and Web Technologies (EIDWT-2019), Fujairah, UAE, 26–28 February 2019; pp. 114–119.
59. Awad, A.; Liu, Y. Cognitive Biometrics for User Authentication. In *Biometric-Based Physical and Cybersecurity Systems*; Obaidat, M.S., Traore, I., Woungang, I., Eds.; Springer International Publishing: London, UK, 2019; pp. 387–399.
60. Belk, M.; Germanakos, P.; Fidas, C.; et al. Studying the Effect of Human Cognition on User Authentication Tasks. In Proceedings of the User Modeling, Adaptation, and Personalization: 21th International Conference, UMAP 2013, Rome, Italy, 10–14 June 2013; pp. 102–113.
61. Perini, I.R.P. Access Control System Using Stimulus Evoked Cognitive Response. U.S. Pat. Appl. US 20140020089A1, 16 January 2014. Available from: https://patentimages.storage.googleapis.com/f3/c9/7e/007a9cbdb91539/US20140020089A1.pdf
62. Di Campi, A.M.; Luccio, F.L. Accessible Authentication Methods for People with Diverse Cognitive Abilities. *Univ. Access Inf. Soc.* **2023**, *24*, 2195–2217.
63. Hayes, J.; Li, X.; Wang, Y. "I Always Have to Think about It First": Authentication Experiences of People with Cognitive Impairments. In Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility, Baltimore, MD, USA, 20 October–1 November 2017; pp. 357–358.
64. Dirks, S.; Bühler, C.; Edler, C.; et al. Cognitive Disabilities and Accessibility—Pushing the Boundaries of Inclusion Using Digital Technologies and Accessible eLearning Environments: Introduction to the Special Thematic Session. In Proceedings of the Computers Helping People with Special Needs: 17th International Conference, ICCHP 2020, Lecco, Italy, 9–11 September 2020; pp. 47–52.
65. Kukawka, A.; Hassan, I.S. System and Method for Cognition-Dependent Access Control. A.U. Pat. Appl. AU 2016291812A1, 16 March 2009.
66. Borina, M.; Kalister, E.; Orehovački, T. Web Accessibility for People with Cognitive Disabilities: A Systematic Literature Review from 2015 to 2021. In Proceedings of the International Conference on Human-Computer Interaction, Online, 26 June–1 July 2022; pp. 261–276.
67. Woods, N.; Siponen, M. Too Many Passwords? How Understanding Our Memory Can Increase Password Memorability. *Int. J. Hum.-Comput. Stud.* **2018**, *111*, 36–48.
68. Al Galib, A.; Safavi-Naini, R. User Authentication Using Human Cognitive Abilities. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; pp. 254–271.
69. Wasfi, H.; Stone, R.; Genschel, U. Word-Pattern: Enhancement of Usability and Security of User-Chosen Recognition Textual Password. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 30–37.
70. Chiasson, S.; Stobert, E.; van Oorschot, P.C.; et al. Multiple Password Interference in Text Passwords and Click-

Based Graphical Passwords. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 500–511.

71. Weinshall, D. Passwords You'll Never Forget, but Can't Recall. In Proceedings of the CHI EA '04: CHI '04 Extended Abstracts on Human Factors in Computing Systems, Vienna Austria, 24–29 April 2004; pp. 1399–1402.
72. Camp, L.J.; Abbott, J.; Chen, S.; et al. Cpasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 3656–3665.
73. Li, B.; Zhou, Q.; Cao, Y.; et al. Cognitively Reconfigurable Mimic-Based Heterogeneous Password Recovery System. *Comput. Secur.* **2022**, *116*, 102667.
74. Shuart, L.H.; Engelhaupt, D.M.; Jankowski, S.E.; et al. Cognitive-Based Logon Process for Computing Device. U.S. Pat. Appl. US 20110162067A1, 15 December 2010.
75. Woods, N.; Siponen, M. Improving Password Memorability, While Not Inconveniencing the User. *Int. J. Hum.-Comput. Stud.* **2019**, *128*, 61–71.
76. Haque, S.T.; Al-Ameen, M.N.; Wright, M.; et al. Learning System-Assigned Passwords (Up to 56 Bits) in a Single Registration Session with the Methods of Cognitive Psychology. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2017), San Diego, CA, USA, 26 February–1 March 2017.
77. Ogiela, M.R.; Ogiela, L. Cognitive Personal Security Systems. In Proceedings of the 13th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2019), Sydney, Australia, 3–5 July 2019; pp. 87–90.
78. McEvoy, P.; Still, J.D. Contextualizing Mnemonic Phrase Passwords. In Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, Orlando, FL, USA, 27–31 July 2016; pp. 295–304.
79. Lahza, H.; Alsamani, B. Behavioral Cybersecurity: Dynamic Persuasive Strategies to Enhance Password Security. In Proceedings of the 2024 7th International Conference of Computer and Informatics Engineering (IC2IE), Bali, Indonesia, 12–13 September 2024; pp. 1–9.
80. Huang, D.; Pal, D. PAAI: Password Authentication Using AI. In Proceedings of the 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Nadi, Fiji, 4–6 December 2023; pp. 1–7.
81. Beck, Z.; Crooks, A.; Rabbi, M.F.; et al. Password Security in Practice: An Appraisal Using Users' Perception and Machine Learning. In Proceedings of the International Conference on Information Technology–New Generations, Las Vegas, NV, USA, 13–16 April 2025; pp. 13–24.
82. Campbell, J.; Ma, W.; Kleeman, D. Impact of Restrictive Composition Policy on User Password Choices. *Behav. Inf. Technol.* **2011**, *30*, 379–388.

Publisher's Note: The views, opinions, and information presented in all publications are the sole responsibility of the respective authors and contributors, and do not necessarily reflect the views of UK Scientific Publishing Limited and/or its editors. UK Scientific Publishing Limited and/or its editors hereby disclaim any liability for any harm or damage to individuals or property arising from the implementation of ideas, methods, instructions, or products mentioned in the content.