A Survey on Password Authentication and Security Mechanisms

www.surveyx.cn

Abstract

Password authentication remains a critical pillar of cybersecurity, serving as the primary method for verifying user identities and securing sensitive data. This survey paper comprehensively examines traditional and modern password authentication mechanisms, highlighting their vulnerabilities and the evolving sophistication of cyber threats. Traditional text-based passwords, while widespread, are fraught with vulnerabilities such as shoulder surfing and social engineering, necessitating the exploration of more secure alternatives like graphical passwords and multi-factor authentication (MFA). The integration of cryptographic methods and artificial intelligence has significantly advanced password security, offering robust defenses against targeted guessing and brute force attacks. This paper also delves into the role of personal information in enhancing guessing attempts and the impact of social engineering and data breaches on password security. Effective defense strategies, including rate limiting, account lockout policies, CAPTCHA, and MFA, are evaluated for their efficacy in mitigating these threats. Furthermore, the survey emphasizes the importance of user-centric design and education in fostering a security-aware culture. By incorporating advanced technologies and focusing on inclusivity, future research can enhance the resilience of authentication systems, ensuring robust protection against emerging cyber threats. The paper concludes with a call for continuous innovation and adaptation in password security practices, underscoring the dynamic nature of cybersecurity challenges and the need for comprehensive strategies to safeguard digital assets.

1 Introduction

1.1 Significance of Password Authentication in Cybersecurity

Password authentication is fundamental to cybersecurity, serving as the primary mechanism for verifying user identities and safeguarding sensitive information. The vulnerabilities of traditional text-based password systems highlight the urgent need for robust authentication methods [1]. As cyber threats increase in sophistication, particularly in sectors with stringent data protection requirements, the limitations of single-password authentication become increasingly evident [2]. This reality emphasizes the necessity for multi-factor authentication (MFA) systems to bolster security.

Inclusivity in the design of security mechanisms is essential for protecting sensitive data across diverse user demographics [3]. To address the weaknesses of traditional alphanumeric passwords, innovative approaches such as graphical password schemes have emerged, designed to mitigate shoulder surfing attacks [4].

Password authentication not only acts as a defensive measure but also constitutes a vital element of a comprehensive cybersecurity strategy. The advancement of authentication methods, including graphical passwords and multifactor authentication systems, is crucial for enhancing the security of digital assets against unauthorized access, particularly in the face of persistent threats like phishing. These innovative strategies improve user experience through techniques such as image-based au-

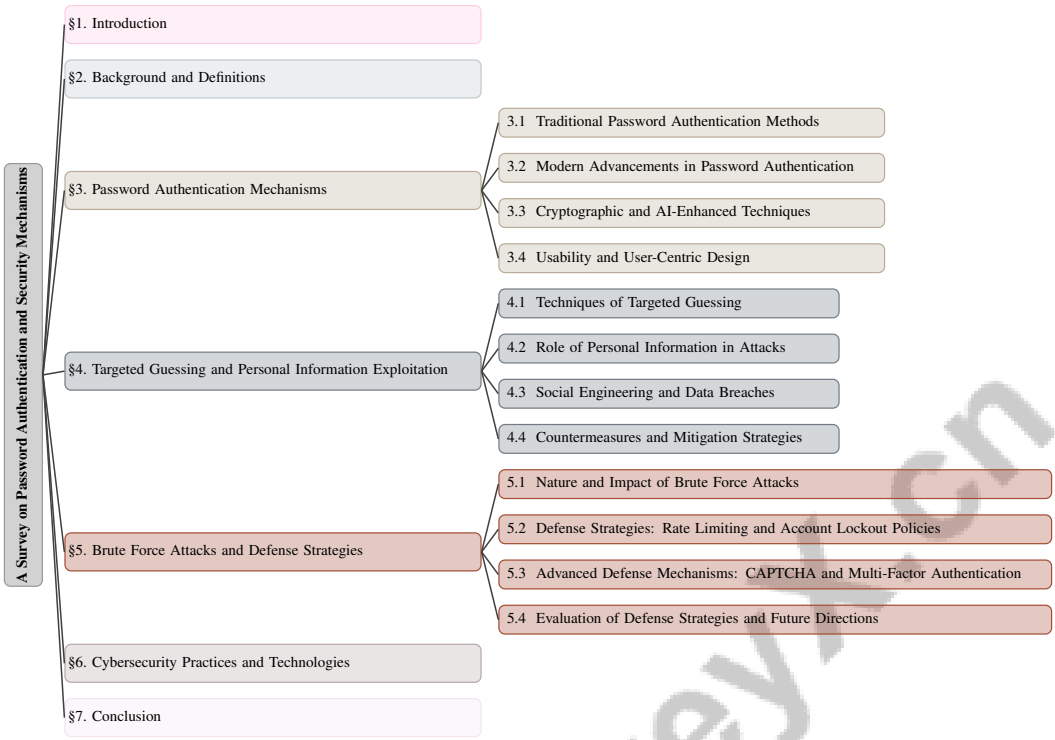


Figure 1: chapter structure

thentication while addressing significant security challenges, thus providing a more resilient defense against emerging cyber threats [5, 6, 7, 8].

1.2 Challenges in Password Authentication

Password authentication systems encounter several challenges that compromise their effectiveness in securing digital identities. A primary concern is the rapid evolution of cyber threats, which often surpass traditional security measures, particularly within complex systems like those in the FinTech sector [9]. The shortcomings of conventional text-based password systems are compounded by vulnerabilities such as shoulder surfing, dictionary attacks, and phishing [1]. Additionally, human-generated passwords are particularly susceptible to guessing attacks, especially in offline scenarios where attackers can leverage substantial computational resources [10].

The challenge of balancing usability and security is particularly pronounced in the design of graphical password systems, which aim to reduce shoulder surfing risks without complicating the authentication process [4]. The increasing sophistication of attacks, such as SIM swapping and stalkerware, further underscores the vulnerabilities in existing two-factor authentication systems [2].

A significant barrier to effective password authentication is the widespread lack of awareness and ingrained behaviors regarding cybersecurity policies among employees, which contribute to vulnerabilities [11]. This lack of awareness is exacerbated by the absence of frameworks that integrate cybersecurity principles into non-security curricula, hindering improvements in cybersecurity education [12].

Moreover, existing benchmarks often neglect the transparency of privacy implications associated with various login options, leading to uninformed user choices [13]. The persistent inadequacies of password-based authentication systems, which remain vulnerable to unauthorized access and attacks, necessitate innovative solutions and comprehensive strategies to enhance both security and usability, ensuring alignment with best practices and regulatory standards.

AI-generated, for reference only.

1.3 Overview of the Paper's Structure

This survey provides a thorough examination of password authentication and security mechanisms, addressing both traditional and contemporary approaches. The introduction outlines the significance of password authentication in cybersecurity, followed by a discussion of the challenges encountered in this area. The second section presents background information and definitions, clarifying key terms such as password authentication, targeted guessing, and brute force attacks, while also offering historical context.

The third section contrasts traditional password authentication methods with modern advancements, assessing their effectiveness against targeted guessing and brute force attacks. This includes an analysis of cryptographic and AI-enhanced techniques, emphasizing the importance of usability and user-centered design.

The fourth section investigates targeted guessing and the exploitation of personal information, discussing how attackers utilize personal data and social engineering to enhance their guessing attempts, alongside strategies to mitigate these risks. The fifth section addresses brute force attacks, evaluating their impact and defense strategies, including rate limiting, account lockout policies, CAPTCHA, and multi-factor authentication.

The sixth section expands the discussion to encompass cybersecurity practices and technologies that support password security, such as password managers, encryption techniques, and machine learning frameworks, highlighting their roles in enhancing overall security. The conclusion summarizes key findings and suggests future research directions.

The survey is informed by existing literature, including a methodology map categorizing password guessing models [14] and a roadmap for discussing tools like Robin for web security [15], ensuring a comprehensive exploration of the topic.The following sections are organized as shown in Figure 1.

2 Background and Definitions

2.1 Key Definitions and Concepts

Understanding key terms is vital in addressing the complexities of password authentication and cybersecurity. Password authentication is a fundamental process for verifying user identity through a secret code, crucial for protecting sensitive information, especially in cloud environments prone to data breaches [16]. Cybersecurity encompasses practices and technologies that safeguard systems, networks, and data from threats, balancing protection with individual rights [17]. Within this framework, password security focuses on creating and managing strong passwords to prevent unauthorized access, underscoring the importance of secure management practices [17].

Attackers often employ targeted guessing techniques, using personal information from social media to predict passwords, highlighting the need for robust protective measures [17]. Brute force attacks systematically attempt to decipher passwords by trying all combinations, emphasizing the importance of complex, lengthy passwords to enhance resistance [15]. Phishing, a prevalent tactic, involves creating fraudulent websites or emails to deceive users into revealing sensitive information, making its recognition and mitigation crucial to cybersecurity strategies [18].

Emerging threats, such as malicious browser extensions and unauthorized access to hardware security keys, demand continuous advancements in authentication technologies [19]. Addressing these threats collaboratively across disciplines is essential for developing effective solutions [9]. Furthermore, organizational culture, policies, training, and leadership significantly influence security compliance, affecting the overall efficacy of cybersecurity measures [11]. In educational contexts, defining essential cybersecurity concepts, such as Capture the Flag (CTF) challenges and their integration into curricula, is crucial for fostering a comprehensive understanding of cybersecurity education [20].

2.2 Historical Context and Evolution

The evolution of password authentication mechanisms reflects broader developments in cybersecurity, adapting to technological advancements and a changing threat landscape. Early systems relied on basic text-based passwords, but as threats grew more sophisticated, these methods became inadequate,

leading to the development of multifactor authentication and innovative graphical password techniques [21, 6, 20, 2].

Password authentication's advancement has been influenced by the evolution of password cracking techniques, categorized by Han [22] into traditional and advanced approaches using technologies like Markov models and linguistic strategies, illustrating the ongoing arms race between cybersecurity practitioners and malicious actors. This trajectory underscores the necessity for continuous innovation in authentication mechanisms to counter emerging threats effectively.

Cybersecurity regulations have critically shaped password authentication practices. Oluomachi [23] highlights how regulations have driven the adoption of stringent authentication protocols, often excluding international and non-cybersecurity-specific policies. The emergence of Password Authenticated Key Exchange (PAKE) protocols, as detailed by Hao [24], marks a significant advancement in securing password exchanges over insecure channels, strengthening the overall security framework.

The historical neglect of marginalized groups in security mechanism development has led to disparities in effectiveness, as noted by Das et al. [3]. This oversight has prompted a reevaluation of authentication technologies to ensure inclusivity and accessibility for diverse users. The evolution of Capture the Flag (CTF) challenges has also significantly contributed to developing cybersecurity skills, transitioning from simple exercises to complex scenarios that provide hands-on experience in addressing real-world issues [20].

The historical development of password authentication reflects efforts to counter sophisticated threats, comply with evolving regulations, and address user inclusivity challenges. This dynamic landscape necessitates ongoing research and innovation to ensure the resilience and effectiveness of authentication systems in protecting digital assets [14, 25].

3 Password Authentication Mechanisms

Category	Feature	Method
Traditional Password Authentication Methods	Network-Based Security	N/A[15]
	Hardware-Based Authentication	RUAS-CD[26]
	Visual-Based Authentication	IBPAS[1]
Modern Advancements in Password Authentication	Usability Enhancement	PBM[27]
Cryptographic and AI-Enhanced Techniques	Data Transformation	HPNN[28]
	Behavioral Analysis	OMEN[10], TCA[29]
	Predictive Modeling	LMDE[30]
	Cryptographic Security	CWEA[16], 2FHA[2]
Usability and User-Centric Design	User Experience Focus	PDIDs[31], SA[32]

Table 1: This table provides a comprehensive overview of various password authentication methods, categorized into traditional approaches, modern advancements, cryptographic and AI-enhanced techniques, and usability-focused designs. Each category lists specific features and methods, illustrating the evolution of authentication mechanisms in response to emerging digital security challenges. The table serves as a valuable resource for understanding the diverse strategies employed to enhance password security.

Examining the limitations of traditional password authentication methods is essential for advancing security measures in the face of increasingly sophisticated digital threats. Traditional methods, primarily text-based passwords, have long been the cornerstone of user authentication but are fraught with vulnerabilities. This section explores these foundational approaches, highlighting their challenges and setting the stage for discussing more secure alternatives. Table 1 presents a detailed categorization of password authentication methods, highlighting the progression from traditional techniques to modern, cryptographic, and AI-enhanced approaches, as well as user-centric designs. Additionally, Table 3 presents a detailed categorization of password authentication methods, emphasizing the transition from traditional techniques to modern, cryptographic, and AI-enhanced approaches, as well as user-centric designs.

To better understand the landscape of password authentication mechanisms, **??** provides a visual representation of their hierarchical structure. This figure categorizes traditional methods alongside modern advancements, cryptographic and AI-enhanced techniques, and usability-focused designs. Each category is meticulously broken down into specific challenges, alternatives, techniques, and approaches, thereby illustrating the evolution and complexity of securing digital identities. By

AI-generated, for reference only.

integrating this visual framework, we can more effectively analyze the shortcomings of traditional methods and the necessity for innovative solutions in the realm of digital security.

3.1 Traditional Password Authentication Methods

Traditional password authentication, reliant on alphanumeric passwords, is prevalent but vulnerable to advanced threats like persistent threats, ransomware, and social engineering [33, 20]. Users often select weak passwords or reuse them across platforms, increasing breach risks. These methods are susceptible to shoulder surfing and social engineering due to predictable user-generated passwords [1]. Protocols like the Yang-Wang-Chang are criticized for vulnerabilities such as replay attacks [26].

Smart card authentication adds security layers but faces challenges in secure password storage and transmission, being vulnerable to server-side attacks [15]. Additionally, traditional methods struggle against advanced password cracking techniques like brute-force attacks [34]. The integration of organizational culture and training into cybersecurity frameworks is limited, affecting efficacy [11, 9].

As illustrated in Figure 2, which highlights the key aspects of traditional password authentication methods, there are significant vulnerabilities and challenges associated with these systems, as well as potential alternatives. The figure emphasizes the urgent need for enhanced security measures in the face of evolving cyber threats. Graphical passwords offer an alternative but often follow predictable patterns that compromise security. They aim to counter shoulder surfing through user-friendly designs but can be cumbersome [4]. The limitations of traditional methods necessitate exploring secure alternatives like Password Authenticated Key Exchange (PAKE) protocols, which enhance security properties [34]. As cyber threats evolve, innovative authentication mechanisms are imperative.

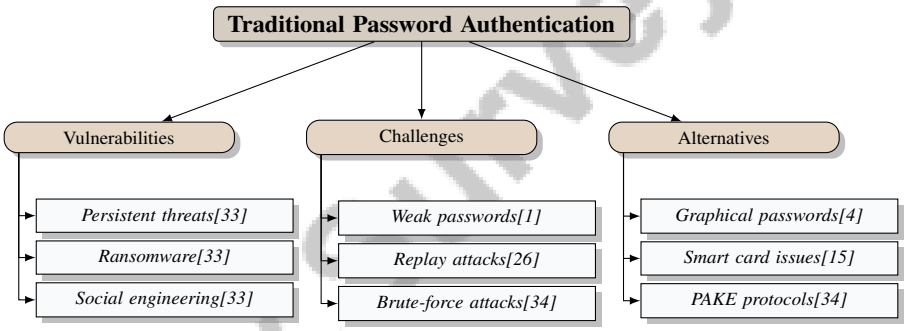


Figure 2: This figure illustrates the key aspects of traditional password authentication methods, highlighting vulnerabilities, challenges, and potential alternatives. It emphasizes the need for enhanced security measures in the face of evolving cyber threats.

3.2 Modern Advancements in Password Authentication

Recent advancements integrate biometric and behavioral methods to enhance security and user convenience. Graphical password systems using game-like interfaces improve resistance to observational attacks [4]. Biometric authentication, incorporating honeytokens, adds defense layers by utilizing unique biological traits [2]. Behavioral methods, like keystroke dynamics and touch-based systems, analyze patterns for personalized security [30, 25].

Auditory stimuli integration, like Baroque music with PassPoints, enhances memorability and usability, though it may increase login time [27]. Sensor-based continuous authentication on smartphones leverages motion patterns and touch gestures for ongoing verification, enhancing security against unauthorized access [35]. These advancements address cybersecurity challenges, including phishing attacks and password vulnerabilities, emphasizing the need for continuous innovation [8, 25].

3.3 Cryptographic and AI-Enhanced Techniques

Cryptography and AI significantly advance password authentication by providing robust defenses against sophisticated threats. Cryptographic techniques, such as Client-side Encryption using Web Assembly, protect data during transmission and storage [16]. The PASTA framework and enhanced

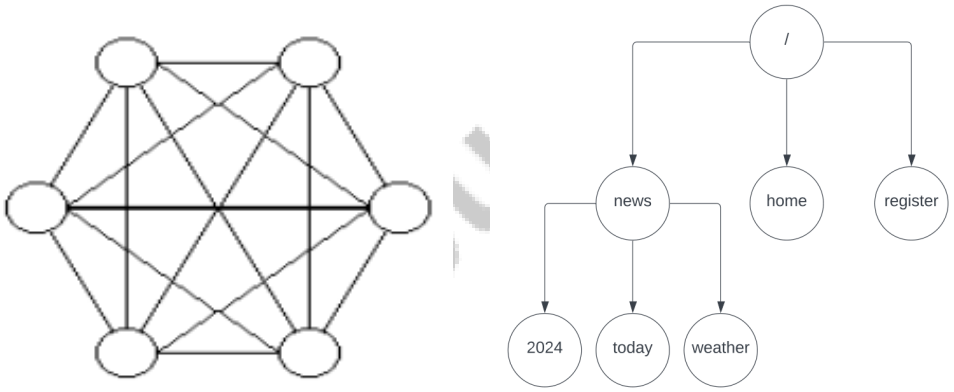
Method Name	Security Techniques	Behavioral Analysis	Integration Methods
CWEA[16]	End-to-end Encryption	User Behaviors	Two Factor Honeytoken
TCA[29]	Cryptographic Applications	Keystroke Dynamics	Two Factor Honeytoken
OMEN[10]	-	-	-
2FHA[2]	Honeytokens	User Behaviors	Honeywords With 2fa
HPNN[28]	Probabilistic Values	-	-
LMDE[30]	-	-	-

Table 2: Overview of Cryptographic and AI-Enhanced Authentication Techniques. This table summarizes various methods, highlighting their use of security techniques, behavioral analysis, and integration methods to enhance password authentication against sophisticated threats.

smartcard-based schemes exemplify cryptographic applications in strengthening authentication [36, 37].

AI enriches authentication by leveraging user behaviors. Sensor-based methods on smartphones combine biometric modalities for enhanced accuracy [35]. Keystroke dynamics, refined through trajectory clustering, identify unique typing patterns [29]. AI methods like OMEN use Markov models to test system robustness [10].

The Two Factor HoneyToken Authentication (2FHA) method combines cryptography and AI, obfuscating authentication tokens to thwart attackers [2]. These advancements address vulnerabilities and pave the way for secure mechanisms, essential in a complex threat landscape [33, 20]. Table 2 provides a comprehensive summary of cryptographic and AI-enhanced techniques used in password authentication, emphasizing their security techniques, behavioral analysis, and integration methods.



(a) The image depicts a geometric figure composed of interconnected circles and lines.[28]

(b) A hierarchical directory structure[30]

Figure 3: Examples of Cryptographic and AI-Enhanced Techniques

As shown in Figure 3, cryptographic and AI-enhanced techniques offer a sophisticated approach to securing digital identities. The geometric figure symbolizes cryptographic networks' complexity, while the hierarchical directory structure represents AI's role in organizing data efficiently. These images underscore the evolving landscape of password authentication, where cryptography and AI enhance security and user experience [28, 30].

3.4 Usability and User-Centric Design

Effective authentication mechanisms require a focus on usability and user-centric design. A user-centric approach incorporates familiar cultural references, enhancing user comprehension and engagement [21]. The PDID method exemplifies user-centric design by simplifying authentication processes [31]. StrongAuth ensures secure communication without compromising user experience [32].

Password managers simplify complex password management, reducing weak password choices [25]. User education and behavioral changes are pivotal, addressing user perceptions and promoting inclusive security practices [17, 3]. Machine learning applications enhance usability by improving

AI-generated, for reference only.

detection rates and aligning security measures with user behaviors [38]. These innovations ensure security measures are both effective and user-friendly.

Feature	Traditional Password Authentication Methods	Modern Advancements in Password Authentication	Cryptographic and AI-Enhanced Techniques
Security Enhancement	Vulnerable TO Attacks	Biometric And Behavioral	Robust Cryptographic Defenses
User Interaction	Alphanumeric Entry	Game-like Interfaces	Ai-driven Behaviors
Technology Integration	Minimal	Sensor-based Systems	Cryptography And AI

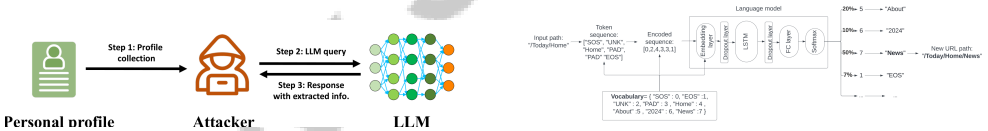
Table 3: This table provides a comprehensive comparison of various password authentication methods, highlighting the evolution from traditional approaches to modern advancements and cryptographic, AI-enhanced techniques. It examines key features such as security enhancement, user interaction, and technology integration, illustrating the progression towards more robust and user-friendly authentication mechanisms.

4 Targeted Guessing and Personal Information Exploitation

4.1 Techniques of Targeted Guessing

Targeted guessing exploits personal information to predict user passwords, capitalizing on the tendency of individuals to use easily accessible details, such as names or birthdates, often shared on social media [10]. Graphical password schemes are particularly vulnerable to shoulder surfing, necessitating more secure design to reduce observational attack risks [4]. Advanced machine learning techniques, including GANs and Markov models, enhance targeted guessing by learning from leaked password databases, improving accuracy by up to 30% [10, 14, 39, 40]. These models analyze user input patterns, predicting passwords more accurately with extensive breach data.

Phishing attacks often employ targeted guessing, tricking users into entering credentials on fake websites. This underscores the need for comprehensive cybersecurity strategies, including robust security measures and employee training, to mitigate risks from advanced threats [33, 12]. Multi-server environments pose additional challenges, as adversaries can impersonate users or create fictitious identities, highlighting the need for user education to safeguard digital identities. Innovative authentication systems and engaging training initiatives, like Capture the Flag challenges, equip users to navigate and mitigate threats to their data [6, 17, 20, 14].



(a) Personal Profile Attack[41]

(b) A diagram illustrating a language model's processing of input text[30]

Figure 4: Examples of Techniques of Targeted Guessing

The examples in Figure 4 illustrate the complexity of targeted guessing, such as the "Personal Profile Attack," which uses language models to exploit personal information. This involves collecting profiles, querying LLMs, and obtaining responses that may contain sensitive data. The diagram shows how a language model processes input text, emphasizing the need for robust security measures to protect against such exploits [41, 30].

4.2 Role of Personal Information in Attacks

Personal information significantly enhances targeted guessing attacks by providing contextual data to predict passwords accurately. Commonly exploited details, such as email addresses and phone numbers, extracted from public profiles, form the basis for precise guessing strategies [41, 10]. Human-originated threats, including insider attacks and social engineering, exacerbate risks by manipulating individuals into revealing credentials or impersonating users, posing challenges to password systems [9]. The lack of emphasis on human aspects like social engineering in educational frameworks highlights the need for enhanced training to mitigate these risks [20].

Despite its potential to improve guessing attack efficiency, personal information integration in password cracking is underutilized. Innovative solutions are needed to address vulnerabilities from personal information exploitation, ensuring robust protection against targeted guessing attacks [10].

4.3 Social Engineering and Data Breaches

Social engineering and data breaches undermine password security by exploiting human vulnerabilities and system weaknesses. Social engineering manipulates individuals into disclosing information through deceptive means, such as phishing emails, exploiting users' trust in familiar interfaces [18]. Data breaches involve unauthorized access to databases, exposing passwords and providing attackers with data to refine password cracking techniques, including targeted guessing [10].

AI amplifies social engineering impact by automating and scaling attacks, making them more efficient and harder to detect. AI analyzes user behavior to craft personalized phishing attacks, boosting success rates and necessitating continuous user education to recognize and respond effectively [17]. Data breaches challenge password systems by enabling credential stuffing attacks, exploiting password reuse, highlighting the importance of robust security measures like multi-factor authentication and password managers [2].

4.4 Countermeasures and Mitigation Strategies

Countering targeted guessing attacks requires a multifaceted approach integrating technology, user education, and inclusive security practices. Strengthening password security involves robust policies mandating complex, unique passwords to mitigate predictability and reuse risks [17]. Cryptographic measures, like client-side encryption, enhance security by protecting data during transmission, addressing vulnerabilities from targeted guessing and breaches [16].

User education is crucial for enhancing password security, raising awareness about risks of easily guessable passwords, and promoting secure practices [3]. Security training for developers is equally important, equipping them to enforce stricter password policies and secure platforms. Collaboration among researchers, practitioners, and regulatory bodies is vital to improve machine learning system robustness against adversarial attacks [35].

Ethical considerations are paramount in cybersecurity strategies, guiding responsible implementation and enhancing public trust. Future research should focus on cohesive ethical guidelines, ensuring technological advancements align with ethical standards [30]. Designing inclusive privacy mechanisms and personalized security training addresses unique challenges faced by diverse user populations, enhancing overall security posture and fostering an inclusive digital environment [3].

5 Brute Force Attacks and Defense Strategies

Brute force attacks exploit authentication system vulnerabilities by systematically guessing passwords through exhaustive combinations, particularly in systems with weak or short passwords, leading to unauthorized access and data breaches [42, 43]. These attacks are especially effective against encrypted databases when executed offline, highlighting vulnerabilities in current authentication systems, including those based on smart cards, necessitating enhanced resistance [44, 45]. Traditional password authentication methods, relying solely on user credentials, are susceptible to these attacks, underscoring the need for more secure mechanisms [46]. Current encryption techniques using pseudo-random number generators can produce weak sequences vulnerable to cryptanalysis, diminishing their effectiveness against brute force attacks [47]. Innovative strategies such as Two Factor HoneyToken Authentication (2FHA) enhance security by integrating honeywords with two-factor authentication, providing robust defense while maintaining user-friendliness [2]. Directory brute-forcing attacks often yield minimal success despite high request volumes, illustrating the challenges associated with brute force strategies [30]. The OMEN system exemplifies advanced techniques capable of cracking approximately 70% of passwords with 10 billion guesses, demonstrating the efficacy of sophisticated password guessers over traditional methods [10]. Dynamic parameters and strict validation processes are essential in mitigating brute force attack risks, preventing replay and impersonation attacks, and enhancing password authentication system security [48]. As cyber threats evolve, the continuous development and adoption of resilient password systems are critical for safeguarding sensitive information.

AI-generated, for reference only.

5.1 Nature and Impact of Brute Force Attacks

Brute force attacks pose a significant threat to password authentication systems by methodically guessing passwords until the correct one is found, exploiting systems that utilize weak passwords and resulting in severe consequences, including unauthorized data access [42, 43]. These attacks can occur both online and offline, particularly when attackers access encrypted password databases. Offline attacks utilize powerful computational resources to crack passwords without online rate limitations [44]. Vulnerabilities in existing authentication systems, particularly smart card-based ones, highlight the need for enhanced defenses against brute force techniques [45]. Traditional methods relying solely on user credentials and one-time passwords are particularly susceptible to brute force attacks, emphasizing the necessity for more secure mechanisms [46]. Current encryption methods relying on pseudo-random number generators may yield weak sequences vulnerable to cryptanalysis, reducing their effectiveness against brute force attacks [47]. Innovative strategies, such as Two Factor HoneyToken Authentication (2FHA), enhance security by integrating honeywords with two-factor authentication, providing robust defense while ensuring user-friendliness [2]. Directory brute-forcing attacks often result in high request volumes with few successful discoveries, illustrating the challenges associated with brute force strategies [30]. The OMEN system, employing advanced techniques, can crack nearly 70% of passwords with 10 billion guesses, showcasing the potential of sophisticated password guessers to outperform traditional methods [10]. Despite advancements, the vast number of possible password combinations and the time required to crack them, particularly with unoptimized methods, remains a significant challenge [42]. Inadequate error messages and notifications often prevent users from detecting local threats, emphasizing the impact of local attacks on password security [49]. To mitigate brute force attack risks, implementing dynamic parameters and strict validation processes is crucial, effectively preventing replay and impersonation attacks and enhancing password authentication system security [48].

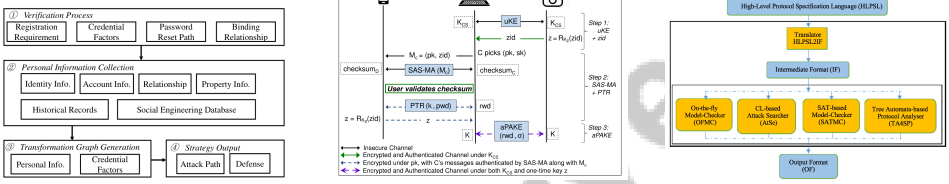
5.2 Defense Strategies: Rate Limiting and Account Lockout Policies

Rate limiting and account lockout policies are fundamental defenses against brute force attacks, restricting login attempts within a specified timeframe. Rate limiting caps user requests, slowing down attackers' ability to execute rapid login attempts, effectively mitigating automated attacks [30]. Account lockout policies complement rate limiting by disabling accounts after a predefined number of unsuccessful attempts, deterring attackers using trial-and-error techniques to guess passwords, significantly lowering unauthorized access likelihood by addressing vulnerabilities in human-generated passwords, which are often weak and based on easily memorable patterns. By leveraging advanced password guessing models, this strategy enhances security and encourages stronger passwords, ultimately mitigating guessing attack risks [10, 14]. Despite their effectiveness, traditional defense mechanisms face challenges, including the increasing sophistication of threats such as advanced persistent threats, ransomware, and social engineering attacks, along with limitations in cross-disciplinary collaboration and standardized terminology [33, 20, 30, 50]. Rate limiting may inadvertently affect legitimate users by introducing delays and reducing overall user experience, particularly in scenarios where users frequently access systems from different locations. Similarly, account lockout policies can be exploited by attackers to lock out legitimate users, creating denial-of-service conditions that disrupt normal operations. Modern implementations of rate limiting and account lockout policies often adopt adaptive strategies that adjust thresholds based on user behavior and historical data, ensuring effectiveness without compromising accessibility. Integrating these mechanisms with advanced monitoring and alerting systems can significantly enhance their effectiveness by providing real-time insights into emerging attack patterns and facilitating immediate responses to suspicious activities [17, 33].

5.3 Advanced Defense Mechanisms: CAPTCHA and Multi-Factor Authentication

Advanced defense mechanisms, including CAPTCHA and multi-factor authentication (MFA), are crucial for fortifying password authentication systems against brute force attacks. CAPTCHA, designed to distinguish between human users and automated bots, presents challenges easy for humans but difficult for machines, effectively thwarting automated brute force attacks [43]. CAPTCHA implementations have evolved to address sophisticated machine learning algorithms attempting to bypass these challenges. Modern CAPTCHA systems incorporate dynamic and interactive elements, such as image recognition or logic puzzles, enhancing robustness against automated attacks [30]. MFA

enhances security by requiring multiple verification forms before granting system access, involving knowledge (e.g., password), possession (e.g., smartphone), and inherence (e.g., biometric data). This multi-factor approach significantly increases the difficulty for attackers to gain unauthorized access, even if one factor is compromised [2]. Integrating MFA into authentication systems has proven effective in mitigating brute force attack risks. By incorporating additional verification steps, MFA fortifies individual accounts and addresses vulnerabilities within the interconnected Online Account Ecosystem, where the security of one account can impact others. Recent studies highlight weaknesses in traditional SMS-based MFA, proposing innovative solutions such as the ActFort system, which evaluates authentication credential factors and interdependencies among online accounts. These advancements underscore the importance of robust MFA in safeguarding sensitive information and protecting users from potential chain reaction attacks [6, 51]. MFA can deter attackers from targeting systems employing these mechanisms, as the increased complexity and time required to bypass MFA make such systems less attractive targets. Despite enhanced security from CAPTCHA and MFA, challenges remain in balancing security with user convenience. CAPTCHA can introduce friction in user experience, particularly for individuals with disabilities or those accessing systems from mobile devices. Similarly, MFA may be perceived as burdensome if the verification process is cumbersome or time-consuming. Organizations are exploring adaptive and context-aware authentication strategies that tailor security measures to the risk level of each transaction, optimizing user experience without compromising security [35].



(a) Verification Process for Personal Information Collection and Strategy Output[51]

(b) The image depicts a secure communication protocol between a mobile device and a laptop, involving a user and a server.[52]

(c) High-Level Protocol Specification Language (HLPSL) Translator System[53]

Figure 5: Examples of Advanced Defense Mechanisms: CAPTCHA and Multi-Factor Authentication

As shown in Figure 5, brute force attacks represent a persistent threat in cybersecurity, necessitating robust defense strategies. Advanced mechanisms like CAPTCHA and MFA play pivotal roles in safeguarding user data and ensuring secure communications. The first figure outlines the verification process for personal information collection, crucial for establishing a secure baseline for user identity management. The second figure emphasizes secure communication protocols, demonstrating the interaction between a mobile device and a laptop through encrypted messages, ensuring data integrity and confidentiality between users and servers. The third figure presents the translation process of a High-Level Protocol Specification Language (HLPSL) into an Intermediate Format, essential for protocol verification and attack detection using advanced tools. Together, these examples underscore the significance of employing multi-layered defense strategies to combat brute force attacks and enhance cybersecurity resilience [51, 52, 53].

5.4 Evaluation of Defense Strategies and Future Directions

Table 4 provides an in-depth examination of representative benchmarks utilized in the evaluation of defense strategies against cybersecurity threats, illustrating the multifaceted nature of current research efforts. Evaluating current defense strategies against brute force attacks reveals both effectiveness and limitations, emphasizing the need for continuous innovation to address emerging threats. Traditional approaches, such as rate limiting and account lockout policies, provide foundational security by restricting login attempts and reducing the likelihood of successful attacks. However, these methods require refinement to mitigate usability issues and the risk of denial-of-service conditions when attackers exploit these policies to lock out legitimate users [42]. Advanced mechanisms like CAPTCHA and MFA have proven effective in enhancing password security. CAPTCHA systems differentiate between human users and automated bots, effectively thwarting automated attacks. Despite their effectiveness,

Benchmark	Size	Domain	Task Format	Metric
PP-Benchmark[54]	12	Cybersecurity	User Authentication	Login Time, Error Rate
LLM-PIE[41]	300	Personal Information Extraction	Information Extraction	Accuracy, Rouge-1
FIDO2[55]	87	Authentication	Usability Testing	SUS, Acceptance Scale
SC-PAP[56]	1,000	Cryptography	Security Analysis	Attack Success Rate, Vulnerability Count
MTB[57]	100,000	Text Classification	Text Classification	F1-score, Accuracy
FIDO2-LA[49]	246,345	Cybersecurity	Security Analysis	Attack Success Rate, User Detection Rate
SA-13[58]	687	Cybersecurity	Survey	Cronbach's alpha, Spearman correlation
SSO-PERM[13]	200	Web Privacy	Login Decision Making	Privacy Preference Shift, Usability Preference Shift

Table 4: This table presents a comprehensive overview of various benchmarks used in cybersecurity and related domains, detailing their respective sizes, domains, task formats, and evaluation metrics. The benchmarks encompass a range of applications from user authentication and personal information extraction to text classification and web privacy, highlighting the diversity and complexity of challenges in the field.

CAPTCHA implementations face challenges in maintaining accessibility, particularly for users with disabilities, necessitating ongoing research to improve usability without compromising security [4]. MFA increases complexity for attackers by requiring multiple verification forms, yet adoption may be hindered by user resistance due to cognitive load [6]. The integration of cryptographic techniques and neural networks in password authentication systems offers promising improvements. Utilizing probabilistic values and neural networks can enhance security by eliminating the need to store passwords on servers, thereby preventing replay attacks and reducing password exposure risk [39]. Additionally, memory-hard functions in password hashing algorithms have shown significant reductions in cracked password percentages, offering both theoretical and practical advantages over existing methods [59]. Despite advancements, challenges persist, particularly from adversarial attacks on keystroke-based authentication methods. The need for improved security measures to counter such attacks is critical, as adversaries increasingly employ advanced techniques to bypass existing defenses [60]. Future research should focus on developing robust models capable of withstanding adversarial influences while maintaining high accuracy and usability [54]. Comparative analyses of Password Authenticated Key Exchange (PAKE) protocols highlight the need for future improvements in defense strategies, particularly in balancing efficiency and security trade-offs [24]. Enhancements in user training and system design could further improve usability and reduce cognitive load, making secure authentication more accessible and user-friendly [6].

6 Cybersecurity Practices and Technologies

In today's cybersecurity landscape, effective practices and technologies are crucial for protecting digital identities and sensitive information. This section delves into key elements that bolster security measures, starting with the role of password managers in enhancing user experience.

6.1 Password Managers and User Experience

Password managers significantly enhance security and user experience by managing complex passwords, thus reducing the cognitive load of remembering multiple credentials. They generate and securely store strong, unique passwords for each account, mitigating the risks associated with password reuse, which can lead to unauthorized access across platforms [25]. Their design, which includes seamless integration across iOS, Android, and desktop platforms, underscores accessibility, enabling users of varying technical expertise to easily store and retrieve encrypted personal data [47].

Despite their benefits, challenges in user education persist, particularly regarding misconceptions about password managers and single sign-on services, highlighting a gap in understanding the security benefits of centralized credential management [25]. Comprehensive education is necessary to build trust in these tools and encourage their adoption.

Integrating password managers with multi-factor authentication (MFA) systems further bolsters security. For instance, the 4FA method, which incorporates multiple authentication factors, exemplifies the

enhanced security achievable through such integration [46]. This combination provides an additional protective layer that is difficult for attackers to bypass, thereby reducing unauthorized access risks.

Innovative systems that simplify login processes, such as those using randomized image grids, eliminate the need for users to remember complex passwords, thus improving user experience [1]. This approach aligns with user-centric design principles, enhancing security while making password management intuitive and less burdensome.

6.2 Encryption Techniques and Secure Data Transmission

Encryption techniques are vital for ensuring data confidentiality and integrity during transmission and storage, forming a core component of cybersecurity frameworks. By converting sensitive information into an unreadable format accessible only with the correct decryption key, encryption protects data from unauthorized access and interception [16]. This is crucial for safeguarding personal data in cloud services, where unauthorized access and data breaches pose significant risks.

Client-side encryption, as demonstrated by the Simple Client-Side Encryption (SCSE) approach, emphasizes encrypting data before it leaves the user's device, ensuring that even if intercepted during transmission, the data remains secure [16]. This method prevents exposure of sensitive information to potentially compromised servers, enhancing the security of data transmission processes.

The integration of cryptographic techniques into password authentication systems underscores encryption's role in securing digital identities. Advanced cryptographic algorithms, such as those in the PASTA framework, protect against server breaches and unauthorized access, ensuring sensitive authentication data remains confidential [36]. This not only enhances password exchange security but also reinforces authentication process integrity.

The evolution of encryption now includes secure transmission of sensitive information across networks, addressing the increased vulnerability of various data types—such as academic records and proprietary designs—to cyberattacks. Secure protocols like Transport Layer Security (TLS) encrypt internet-transmitted data, protecting it from eavesdropping and tampering by malicious actors, which is crucial for safeguarding sensitive transactions [17, 8].

6.3 Machine Learning and Cybersecurity Frameworks

Machine learning (ML) is integral to enhancing cybersecurity frameworks, particularly in password security. By analyzing extensive datasets and identifying intricate patterns, ML provides innovative solutions for safeguarding digital identities and fortifying authentication mechanisms. A notable application is the use of deep learning techniques, such as recurrent neural networks, to detect malicious URLs and enhance password security, as demonstrated by the Phish-Defence system [18]. This system illustrates ML's capability to proactively identify threats and prevent phishing attacks, common precursors to password breaches.

ML integration extends to developing robust authentication methods. For instance, extended chaotic map-based Diffie-Hellman problems in ML-driven systems illustrate the potential for creating secure session keys that ensure both users and servers contribute to the generation process, thus enhancing overall security [37]. This adaptability of ML refines authentication protocols, ensuring resilience against evolving cyber threats.

Future advancements in ML-driven cybersecurity frameworks may incorporate a wider range of biometric features, such as facial recognition, fingerprint scanning, and behavioral biometrics, to enhance authentication robustness. This evolution aims to address the limitations of traditional password-based methods, which often compromise security or usability. By leveraging advanced biometric modalities, organizations can better defend against sophisticated cyber threats, including personal information extraction techniques highlighted in recent studies, while improving user experience and reducing unauthorized access risks [6, 38, 41]. Exploring common datasets for keystroke analysis and other biometric modalities could lead to comprehensive security solutions that are user-friendly and resistant to both classical and quantum attacks, particularly as quantum computing necessitates improvements in the security and efficiency of Password Authenticated Key Exchange (PAKE) protocols.

ML integration underscores the need for collaboration among diverse stakeholders—including researchers, practitioners, and policymakers—to bridge the gap between research and practical application. This collaboration is essential for maximizing ML's advantages over traditional human-driven detection methods and addressing intrinsic challenges that hinder effective ML deployment in cybersecurity. By fostering interdisciplinary communication and standardizing cybersecurity terminology, stakeholders can enhance mutual understanding and cooperation, ultimately advancing ML technologies to defend against evolving cyber threats [50, 38]. By leveraging ML's analytical capabilities, cybersecurity practitioners can develop sophisticated and resilient authentication mechanisms that effectively safeguard digital assets, ensuring strategies align with best practices to address emerging threats.

6.4 User Education and Behavioral Aspects

User education and behavioral changes are pivotal in enhancing cybersecurity, particularly for populations lacking adequate knowledge of security practices [3]. Integrating user education into cybersecurity strategies is essential for fostering a culture of awareness and resilience against cyber threats. This is particularly relevant in the context of Capture the Flag (CTF) challenges, which impart practical skills and knowledge vital for navigating the cybersecurity landscape [20].

User education extends beyond traditional training, emphasizing the importance of transparency in login options and the influence of displaying permission-related information on user behavior. Such transparency can lead to better design practices in web single sign-on (SSO) systems, ultimately enhancing user trust and security [13]. By equipping users with the necessary knowledge to make informed decisions, organizations can significantly reduce vulnerabilities associated with uninformed user choices.

Advancements in graphical password security have improved user engagement and memorability, making these systems more user-friendly and effective against shoulder surfing attacks [4]. However, reliance on smartphones or SMS capabilities for certain authentication methods, such as those involving honeytokens, poses challenges for users without access to such technologies, particularly the elderly [2].

7 Conclusion

This survey delves into the complexities of password authentication and security mechanisms, highlighting the indispensable role of cryptographic methods and artificial intelligence in fortifying defenses against sophisticated cyber threats. The progression in behavioral biometrics offers a viable path for continuous authentication, effectively marrying usability with security, a synergy often absent in conventional approaches. Image-based password systems emerge as a forward-thinking solution, addressing vulnerabilities inherent in traditional password paradigms.

The current cybersecurity landscape necessitates a focus on user-centric design, integrating human factors into security strategies to accommodate diverse user requirements and enhance protective measures. The influence of user awareness, attitudes, and knowledge on the perceived usability of cybersecurity protocols underscores the imperative for future research to engage users actively and promote the adoption of secure practices.

Future research trajectories might explore the refinement of personal information integration into password cracking methodologies and the development of advanced models that consider varied password creation behaviors. Enhancing authentication schemes for mobile platforms and incorporating biometric verification could further bolster user protection. The potential of trajectory clustering techniques in authenticating users via keystroke dynamics presents a promising alternative to traditional password systems.

The integration of advanced real-time phishing detection systems into cybersecurity frameworks is crucial, as exemplified by systems like Phish-Defence. Addressing human factors in cybersecurity requires a comprehensive approach that blends technological advancements with behavioral insights. Future investigations should encompass broader user demographics and examine the long-term implications of providing permission-related information on login choices.

Despite notable advancements in password authentication and security, ongoing innovation and adaptability are essential to counteract the evolving nature of cyber threats. By emphasizing inclusivity, user-focused design, and the incorporation of cutting-edge technologies, future research can enhance the development of robust authentication systems, ensuring the protection of digital assets in a dynamic threat environment. Exploring hybrid models that integrate graphical and textual elements could strengthen defenses against shoulder surfing attacks. Furthermore, the secure deployment of protocols like CPace, particularly in quantum-resistant contexts, remains a pivotal area for future investigation. Finally, insights from CTF challenges suggest that future research should integrate human-centric topics alongside technical expertise.

References

[1] Sanjida Akter Sharna and Sheikh Ashraf Ali. Image based password authentication system, 2022.

[2] Vasilis Papaspirou, Maria Papathanasaki, Leandros Maglaras, Ioanna Kantzavelou, Christos Douligeris, Mohamed Amine Ferrag, and Helge Janicke. Cybersecurity revisited: Honeytokens meet google authenticator, 2021.

[3] Sanchari Das, Robert S. Gutzwiller, Rod D. Roscoe, Prashanth Rajivan, Yang Wang, L. Jean Camp, and Roberto Hoyle. Panel: Humans and technology for inclusive privacy and security, 2021.

[4] Arash Habibi Lashkari, Samaneh Farmand, Dr. Omar Bin Zakaria, and Dr. Rosli Saleh. Shoulder surfing attack in graphical password authentication, 2009.

[5] Jinyong Chen, Reiner Dojen, and Anca Jurcut. Detection and prevention of new attacks for id-based authentication protocols, 2021.

[6] Gloriya Mathew and Shiney Thomas. A novel multifactor authentication system ensuring usability and security, 2013.

[7] Teik Guan Tan, Pawel Szalachowski, and Jianying Zhou. Securing password authentication for web-based applications, 2020.

[8] Sanjay Majumder, Sanjay Chakraborty, and Suman Das. A new advanced user authentication and confidentiality security service, 2014.

[9] Danial Javaheri, Mahdi Fahmideh, Hassan Chizari, Pooia Lalbakhsh, and Junbeom Hur. Cybersecurity threats in fintech: A systematic review, 2023.

[10] Claude Castelluccia, Abdelberi Chaabane, Markus Dürmuth, and Daniele Perito. When privacy meets security: Leveraging personal information for password cracking, 2013.

[11] Sarah Sharifi. A novel approach to the behavioral aspects of cybersecurity, 2023.

[12] Mohammad Azzeh, Ahmad Mousa Altamimi, Mahmood Albashayreh, and Mohammad A AL-Oudat. Adopting the cybersecurity concepts into curriculum the potential effects on students cybersecurity knowledge, 2022.

[13] Srivathsan G. Morkonda, Sonia Chiasson, and Paul C. van Oorschot. Influences of displaying permission-related information on web single sign-on login decisions, 2023.

[14] Lam Tran, Thuc Nguyen, Changho Seo, Hyunil Kim, and Deokjai Choi. A survey on password guessing, 2022.

[15] Guilherme Girotto and Avelino Francisco Zorzo. Robin: A web security tool, 2020.

[16] Marco Falda and Angela Grassi. Simple client-side encryption of personal information with web assembly, 2023.

[17] Ahmad Reda Alzighaibi. Cybersecurity attacks on academic data and personal information and the mediating role of education and employment. *Journal of Computer and Communications*, 9(11):77–90, 2021.

[18] Aman Rangapur, Tarun Kanakam, and Dhanvanthini P. Phish-defence: Phishing detection using deep recurrent neural networks, 2022.

[19] Maria Bada and Basie von Solms. A cybersecurity guide for using fitness devices, 2021.

[20] Valdemar Švábenský, Pavel Čeleda, Jan Vykopal, and Silvia Brišáková. Cybersecurity knowledge and skills taught in capture the flag challenges, 2021.

[21] Luca Viganò. Explaining cybersecurity with films and the arts (extended abstract), 2019.

[22] Lifeng Han. Password cracking and countermeasures in computer security: A survey, 2023.

[23] Ejiofor Oluomachi, Akinsola Ahmed, Wahab Ahmed, and Edozie Samson. Assessing the effectiveness of current cybersecurity regulations and policies in the us, 2024.

[24] Feng Hao and Paul C van Oorschot. Sok: password-authenticated key exchange–theory, practice, standardization and real-world lessons. In *Proceedings of the 2022 ACM on Asia conference on computer and communications security*, pages 697–711, 2022.

[25] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):1–32, 2018.

[26] Amit K Awasthi. A new remote user authentication scheme using smart cards with check digits, 2005.

[27] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, and Uwe Aickelin. The effect of baroque music on the passpoints graphical password, 2013.

[28] ASN Chakravarthy, P S Avadhani, P. E. S. N Krishna Prasad, N. Rajeevand, and D. Rajasekhar Reddy. A novel approach for authenticating textual or graphical passwords using hopfield neural network, 2011.

[29] Hazarath Munaga, J. V. R. Murthy, and N. B. Venkateswarlu. Enhanced user authentication through trajectory clustering, 2011.

[30] Alberto Castagnaro, Mauro Conti, and Luca Pajola. Offensive ai: Enhancing directory brute-forcing attack with the use of language models, 2024.

[31] Pawel Szalachowski. Password-authenticated decentralized identities. *IEEE Transactions on Information Forensics and Security*, 16:4801–4810, 2021.

[32] Yassine Sadqi, Ahmed Asimi, and Younes Asimi. A cryptographic mutual authentication scheme for web applications, 2014.

[33] Daksh Dave, Gauransh Sawhney, Pushkar Aggarwal, Nitish Silswal, and Dhruv Khut. The new frontier of cybersecurity: Emerging threats and innovations, 2023.

[34] Edward Eaton and Douglas Stebila. The "quantum annoying" property of password-authenticated key exchange protocols. In *Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12*, pages 154–173. Springer, 2021.

[35] Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey, 2020.

[36] Shashank Agrawal, Peihan Miao, Payman Mohassel, and Pratyay Mukherjee. Pasta: password-based threshold authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 2042–2059, 2018.

[37] Tian-Fu Lee, Chia-Hung Hsiao, Shi-Han Hwang, and Tsung-Hung Lin. Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps. *Plos one*, 12(7):e0181744, 2017.

[38] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Burdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. The role of machine learning in cybersecurity, 2022.

[39] ASN Chakravarthy and Prof. P S Avadhani. A probabilistic approach for authenticating text or graphical passwords using back propagation, 2011.

[40] Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, and Fernando Perez-Cruz. Passgan: A deep learning approach for password guessing. In *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17*, pages 217–237. Springer, 2019.

[41] Yupei Liu, Yuqi Jia, Jinyuan Jia, and Neil Zhenqiang Gong. Evaluating llm-based personal information extraction and countermeasures, 2025.

[42] Enrico Siviero. Password cracking and tools: Analysis of automatic cracking tools and password guessing. 2023.

[43] Muhammad Shoaib Farooq and Hina jabbar. Phishing website detection using a combined model of ann and lstm, 2024.

[44] Yalin Chen, Jue-Sam Chou*, and Chun-Hui Huang. Comments on five smart card based password authentication protocols, 2010.

[45] A. S. N. Chakravarthy, Penmetsa V. Krishna Raja, and Prof. P. S. Avadhani. A novel approach for password authentication using bidirectional associative memory, 2011.

[46] Sanyam Jain, Raju gautam, Shivani Sharma, and Ravi Tomar. Four factor authentication with emerging cybersecurity for mobile transactions, 2023.

[47] Victor Solovyev and Ramzan Umarov. Fendoff encryption software to secure personal information on computers and mobile devices, 2015.

[48] Al-Sakib Khan Pathan and Choong Seon Hong. An improved timestamp-based password authentication scheme using smart cards, 2007.

[49] Tarun Kumar Yadav and Kent Seamons. A security and usability analysis of local attacks against fido2, 2023.

[50] Robert Ramirez and Nazli Choucri. Improving interdisciplinary communication with standardized cyber security terminology: A literature review, 2020.

[51] Weizhao Jin, Xiaoyu Ji, Ruiwen He, Zhou Zhuang, Wenyuan Xu, and Yuan Tian. Sms goes nuclear: Fortifying sms-based mfa in online account ecosystem, 2021.

[52] Stanislaw Jarecki, Hugo Krawczyk, Maliheh Shirvanian, and Nitesh Saxena. Two-factor authentication with end-to-end password security. In *Public-Key Cryptography–PKC 2018: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II 21*, pages 431–461. Springer, 2018.

[53] Shuming Qiu, Guoai Xu, Haseeb Ahmad, and Yanhui Guo. An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy. *PloS one*, 13(3):e0194072, 2018.

[54] Ignacio Astaburuaga. User study: Comparison of picture passwords and current login approaches, 2024.

[55] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. Fido2 the rescue? platform vs. roaming authentication on smartphones, 2023.

[56] Juan E. Tapiador, Julio C. Hernandez-Castro, P. Peris-Lopez, and John A. Clark. Cryptanalysis of song's advanced smart card based password authentication protocol, 2011.

[57] Hala Assal, Ahsan Imran, and Sonia Chiasson. An exploration of graphical password authentication for children, 2016.

[58] Cori Faklaris, Laura Dabbish, and Jason I. Hong. Do they accept or resist cybersecurity measures? development and validation of the 13-item security attitude inventory (sa-13), 2022.

[59] Wenjie Bai, Jeremiah Blocki, and Mohammad Hassan Ameri. Cost-asymmetric memory hard password hashing, 2022.

[60] Idoia Eizaguirre-Peral, Lander Segurola-Gil, and Francesco Zola. Conditional generative adversarial network for keystroke presentation attack, 2022.

Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.