JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 36 (2025) 328–335
Received: 9 May 2025
Accepted: 22 June 2025

Password Managers: A Critical Review of Security, Usability, and Innovative Designs

Menadżery haseł: krytyczny przegląd bezpieczeństwa, użyteczności i innowacyjnych projektów

Hussein Abdulkhaleq Saleh*

Directorate General of Education in Dhi Qar, Al-Haboubi Street, Nasiriyah, 64001, Dhi Qar, IRAQ.

Abstract

Password managers are crucial for securely managing online credentials in today's digital landscape. This review synthesizes insights from 25 research papers to evaluate current password management systems, focusing on their approaches to security, usability, and innovation. We explore strategies to counter security challenges such as offline attacks, phishing, and device compromise, as well as efforts to enhance usability through intuitive interfaces and simplified authentication. The review also analyzes innovative architectural designs and cryptographic techniques that underpin these systems. Our synthesis highlights significant advancements in creating secure, resilient, and user-friendly password managers, while identifying gaps in usability testing, scalability of distributed systems, and cryptographic standardization. This comprehensive overview provides critical insights and directions for future research to optimize the balance between security and usability in password management.

Keywords: Password managers; Security; Usability; Cryptography

Streszczenie

Menadżery haseł są kluczowe dla bezpiecznego zarządzania poświadczeniami online w dzisiejszym cyfrowym krajobrazie. Ten przegląd syntetyzuje wnioski z 25 prac badawczych, aby ocenić obecne systemy zarządzania hasłami, koncentrując się na ich podejściach do bezpieczeństwa, użyteczności i innowacji. Badamy strategie przeciwdziałania wyzwaniom bezpieczeństwa, takim jak ataki offline, phishing i kompromitacja urządzeń, a także wysiłki na rzecz poprawy użyteczności poprzez intuicyjne interfejsy i uproszczone uwierzytelnianie. Przegląd analizuje również innowacyjne projekty architektoniczne i techniki kryptograficzne, które leżą u podstaw tych systemów. Nasza synteza podkreśla znaczące postępy w tworzeniu bezpiecznych, odpornych i przyjaznych dla użytkownika menadżerów haseł, jednocześnie identyfikując luki w testowaniu użyteczności, skalowalności systemów rozproszonych i standaryzacji kryptograficznej. Ten kompleksowy przegląd dostarcza kluczowych wniosków i kierunków dla przyszłych badań, aby zoptymalizować równowagę między bezpieczeństwem a użytecznością w zarządzaniu hasłami.

Słowa kluczowe: Password managers; Security; Usability; Cryptography

*Corresponding author

Email address: hussein.abd.alkhaliq@cgmail.com (H. A. Saleh)

1. Introduction

In today's digital landscape, passwords serve as the cornerstone of security for countless online services, including banking, social media, and e-commerce. As users juggle an ever-increasing number of accounts, managing these credentials securely has become a daunting task. Studies reveal that users frequently resort to insecure practices (such as reusing passwords across multiple sites, choosing weak passwords, or storing them unsafely) due to the difficulty of memorizing complex, unique credentials for each account [1]. These habits heighten the risk of breaches, identity theft, and data compromise, particularly as cyber threats like phishing and credential stuffing grow more sophisticated.

Password managers have emerged as an essential solution to address these challenges, enabling users to generate, store, and retrieve strong, unique passwords with ease. By reducing the cognitive load on users, these systems promote secure practices while offering convenience. The field has seen significant evolution, with designs ranging from traditional vault-based systems that encrypt passwords locally or in the cloud to advanced approaches like generative models that create passwords on demand and distributed architectures that avoid single points of failure [2]. Despite their advantages, password managers face their own hurdles, including vulnerabilities to attacks on stored credentials, reliance on a master password, and usability barriers that hinder widespread adoption [3].

This review synthesizes findings from 25 research papers to explore the current state of password management. These papers span a wide array of topics, including security mechanisms, usability enhancements, and innovative designs such as hardware integration and biometric authentication. The analysis focuses on how these systems balance security and usability, identifying key advancements and persistent challenges. By examining this body of work, this paper aims to provide a comprehensive overview and guide future efforts in developing effective password management solutions.

2. Background

Password managers have become widely adopted tools in the modern digital landscape, addressing the growing challenge of managing multiple, complex passwords across various online services. As cyber threats evolve, so too have the designs and capabilities of password managers, reflecting a continuous effort to balance security and usability. This section provides a brief history of password managers, outlines the common types currently in use, and highlights the key security and usability issues that have shaped their development.

2.1. Brief History of Password Managers

The concept of password management emerged alongside the proliferation of online services in the late 20th century. Early password managers were simple vault-based systems that stored encrypted passwords locally on a user's device or in the cloud. These systems relied on a single master password to unlock the vault, providing a convenient way to store and retrieve credentials [4]. However, as cyber threats like data breaches and phishing attacks became more sophisticated, the limitations of these early designs became apparent. Vulnerabilities such as weak master passwords and the risk of offline attacks on stored vaults prompted the development of more advanced solutions [5].

In response, researchers and developers began exploring generative approaches that create passwords on demand without storing them, thereby eliminating the risk of vault compromise [6]. Other innovations included the integration of hardware components, such as Physically Unclonable Functions (PUFs) [7] and USB keys [8], to add layers of security. Additionally, the rise of multi-device usage led to the creation of distributed password managers that split secrets across devices, reducing the risk associated with single points of failure [9-11]. Today, password managers continue to evolve, incorporating biometric authentication [17, 12] and cloud-based synchronization [13-15] to meet the demands of modern users.

2.2. Common Types of Password Managers

In this review, passwords refer to…" is clear but could read slightly more smoothly as "In this review, we use 'passwords' to mean user-chosen authentication strings, and 'secrets' for cryptographic keys or shares in distributed systems. Password managers can be broadly categorized into several types based on their design and functionality:

- Vault-based managers: These are the most traditional form of password managers, storing encrypted passwords in a secure vault that is accessible via a master password. The vault can be stored locally on the user's device or in the cloud, with popular examples including LastPass, KeePass, and the systems described in [13-21]. While convenient, these managers are vulnerable to attacks if the master password is weak or if the vault is compromised.
- Generative managers: Instead of storing passwords, generative managers use algorithms to create unique, site-specific passwords on demand. These systems typically require a master password and additional inputs, such as the website's name, to generate consistent passwords across devices without the need for storage [2, 6, 9, 22-25]. This approach significantly reduces the risk of password theft but may require users to remember additional information, such as hints or metadata.
- Distributed or multi-device managers: These systems enhance security by distributing password shares across multiple devices, ensuring that no single device holds the complete password. Examples include [9-11, 25], which use techniques like Shamir's Secret Sharing or bilateral generation to protect against device compromise. While offering robust security, these managers often require network connectivity and can be more complex to use.
- Hardware-integrated managers: By incorporating hardware components such as PUFs [7] or USB keys [8], these managers add an extra layer of security tied to the physical device. This makes it significantly harder for attackers to access passwords without the specific hardware, though it may limit portability and convenience.

2.3. Key Security and Usability Issues

Despite their benefits, password managers face several persistent challenges that impact their security and usability:

- Security Issues:
  - Vulnerability to offline attacks: If an attacker gains access to the stored vault or password shares, they may attempt to crack the master password or decrypt the data through offline brute-force attacks [2, 7, 16, 21, 25, 26]. This risk is particularly acute for vault-based managers.
  - Phishing attacks: Users may be tricked into entering their credentials on fraudulent websites, a threat that some managers mitigate through domain verification or URL matching [2, 19, 22, 25, 28].
  - Device compromise: If a user's device is stolen or infected with malware, the security of the passwords can be compromised. Solutions like distributed systems and hardware integration aim to address this by ensuring that no single device holds all the necessary information [7-11].
- Usability Issues:
  - Cognitive load: The need to remember multiple complex passwords or additional inputs (e.g., hints) can be burdensome for users, leading to

insecure practices such as password reuse or weak password choices [6, 13-16].

- User adoption barriers: Many users are deterred by the perceived complexity of password managers, lack of trust in their security, or inconvenience of setup and use [3, 21-23]. Simplifying interfaces and improving user education are critical to increasing adoption.
- Synchronization and accessibility: Ensuring that passwords are securely synchronized across multiple devices without compromising security remains a challenge, particularly for cloud-based solutions [10,13-15, 20].

These security and usability issues have driven much of the innovation in password management, as researchers and developers seek to create systems that are both highly secure and user-friendly. The following sections will explore how various approaches have attempted to address these challenges, highlighting the trade-offs and advancements in the field.

3. Methodology

This review undertakes an analysis of 25 pre-selected research papers, provided to the author, focused on the topic of password managers. The set of these 25 papers was fixed for the purpose of this review; consequently, no external databases (e.g., IEEE Xplore, ACM Digital Library, Scopus) were searched, and no additional papers were selected by the author beyond this initial corpus. The primary objective was to synthesize the findings from this specific collection of literature. The review process involved a thorough examination of each summary to identify the primary contributions, methodologies detailed (if any), and key findings presented in the papers. No additional primary research or literature searches were conducted beyond the analysis of the provided papers; the review relies solely on the information presented therein.

While the selection of papers was predetermined for this review, precluding a PRISMA-guided search and selection process, the subsequent analysis of the provided papers was conducted systematically. This systematic process involved a consistent data extraction approach for each summary, focusing on identifying the core problem addressed, the proposed solution, the methodology employed (if detailed in the summary), key findings, and notable security or usability implications. Following this extraction, a thematic analysis was performed. The papers were categorized into four main thematic areas based on their primary focus, as determined by the main problem addressed or the key contribution highlighted in the summary:

- Addressing Security Challenges (covered in Section 4.1)
- Enhancing Usability and Adoption (covered in Section 4.2)
- Innovative Architectural Designs (covered in Section 4.3)
- Cryptographic Techniques and Protocols (covered in Section 4.4)

For instance, papers proposing solutions to mitigate offline attacks were grouped under ‘Addressing Security Challenges,’ while those introducing user-interface improvements were placed under ‘Enhancing Usability and Adoption.’ Some papers addressed multiple aspects and were referenced accordingly in the relevant sections. The synthesis of findings involved identifying common trends, divergent approaches, and existing gaps within this defined set of 25 papers. We acknowledge that a broader literature search using PRISMA guidelines would typically be part of a comprehensive systematic review; however, this study was constrained to the analysis of the provided set of papers.

4. Main Body

4.1. Addressing Security Challenges

4.1.1.Mitigating Offline Attacks

Offline attacks represent a critical vulnerability for password managers, as attackers can attempt to decrypt stolen credential vaults without detection. 6 of the 25 reviewed papers (24%) proposed innovative solutions to counter this threat. Generative approaches eliminate the need for password storage entirely, reducing the risk of offline exploitation. For instance, [2] introduces HIPPO, a cloud-based password manager that uses Device-Enhanced Password Authenticated Key Exchange (DE-PAKE) to generate passwords on demand, ensuring no stored credentials are available for attackers to target. However, its cloud-based nature may introduce latency or dependency on internet access, potentially affecting usability in low-connectivity scenarios. Similarly, [25] presents SPHINX, which employs DE-PAKE to compute high-entropy passwords without storing them, thwarting offline dictionary attacks even if the device is compromised.

Hardware-based defences provide another layer of protection. [7] proposes PUFPass, leveraging Physically Unclonable Functions (PUFs) to generate unique passwords tied to specific hardware, making offline replication impractical without the original device.

Distributed systems further enhance security by fragmenting sensitive data across multiple entities. [10] describes NoKey, which uses Shamir's Secret Sharing to split a 256-bit AES encryption key into shares distributed across user devices, requiring a threshold of shares to reconstruct the key and preventing offline attacks unless multiple devices are breached. Likewise, [11] introduces SplitPass, splitting passwords between a user’s device and a cloud assistant, ensuring neither entity holds the complete credential. These strategies (generative, hardware-based, and distributed) collectively demonstrate a robust response to offline attack vulnerabilities. Another approach to mitigating offline attacks is to conceal the encrypted data itself. Ahuja et al. [27] introduce a password manager that encrypts credentials using Blowfish and then hides the ciphertext within images using LSB steganography, making it more difficult for attackers to locate and target the encrypted data. By embedding the encrypted credentials within images using LSB steganography, this method ensures that even if an attacker gains access to the device, they may not realize that sensitive data is present, thereby reducing the likelihood of an offline attack. This dual-layer security approach exemplifies how combining cryptographic techniques with data hiding can enhance protection against unauthorized access.

4.1.2.Phishing Resistance

Phishing attacks exploit user trust by tricking them into entering credentials on fraudulent websites, a persistent challenge for password security. 5 of the 25 reviewed papers (20%) discussed mechanisms to resist such threats. Password managers have developed mechanisms to resist such threats, often by tying credentials to verified domains or URLs. [2] (HIPPO) incorporates domain verification into its password generation process, ensuring passwords are only valid for legitimate sites. Similarly, [25] (SPHINX) computes passwords using domain names, inherently resisting phishing by rendering the credentials useless on fake sites.

Additional systems enhance protection through explicit verification techniques. [22] (Versipass) employs URL verification to confirm website authenticity before releasing passwords, while [19] (Online Safe Vault) uses a greeting mechanism to validate the host, displaying a customized message to reassure users of legitimacy. [28] leverages CardSpace’s PassCards, optionally including website URLs to match against login pages, providing an extra safeguard against phishing. These approaches collectively aim to protect users by ensuring credentials are only disclosed to verified, legitimate destinations.

4.1.3.Device Compromise Resilience

Device compromise—through theft, malware, or unauthorized access—poses a significant risk to password manager security, and strategies to enhance resilience were detailed in 5 of the 25 reviewed papers. Distributed architectures mitigate this by avoiding single points of failure. [9] (Amnesia) distributes secrets between a server and a smartphone, requiring both to generate passwords, so compromising one device alone is insufficient for access. [10] (NoKey) further advances this concept by splitting encryption keys across multiple devices using Shamir's Secret Sharing, ensuring resilience unless a threshold of devices is breached. While NoKey [10] enhances security through distributed key shares, its reliance on multiple devices may complicate setup and use, particularly in scenarios with limited connectivity.

Hardware integration offers complementary protection. [8] employs a USB key to store the private key for RSA encryption, necessitating physical possession for access. [7] (PUFPass) binds passwords to specific hardware via PUFs, preventing replication on other devices. [11] (SplitPass) splits passwords between a device and a cloud assistant, ensuring neither holds the full credential, thus requiring simultaneous compromise of both. These methods—distributing trust and leveraging physical components—enhance resilience against device-specific threats. Having explored the security challenges and solutions, the next section shifts focus to usability enhancements, which are equally critical for the widespread adoption of password managers.

4.2. Enhancing Usability and Adoption

4.2.1.User Interface and Experience Improvements

Usability is pivotal for widespread adoption, and 4 of the 25 reviewed papers (16%) focused on designing intuitive systems or improving user interfaces to reduce cognitive load. [22] (Versipass) uses image cues and category models to improve memorability and account association, harnessing visual memory to simplify password recall. [3] (ByPass) integrates directly with websites via APIs, streamlining tasks like registration and login, minimizing user effort and errors.

Other efforts prioritize seamless functionality. [20] (SAFEPASS) offers a user-friendly interface with features like password generation and cloud synchronization, enhancing accessibility. [21] proposes a cloud-based, storage-free BPM with a secure UI for master password entry, balancing security, and ease of use. These advancements aim to make password managers more approachable, addressing a key barrier to adoption.

4.2.2.Simplifying Authentication

Authentication complexity often hinders user experience, and innovations to streamline access were explored in 20% of the reviewed papers. [17] (BANK OF PASSWORDS) incorporates fingerprint authentication alongside a master password, offering a convenient biometric alternative. [12] enhances security with privacy-preserving biometrics as part of two-factor authentication, simplifying access without sacrificing protection.

More radical designs eliminate traditional master passwords. [23] (MonoPass) uses the master password solely for password generation, not access, relying on metadata synchronization instead. [10] (NoKey) removes the master password entirely, using device-based key shares for authentication. These approaches reduce authentication friction, making password managers more appealing to users. ByPass [3] streamlines authentication by integrating directly with websites via APIs, akin to single sign-on (SSO) principles, thereby reducing user actions during login.

4.2.3.Encouraging Secure Behaviour

Password managers can guide users toward secure practices, and 12% of the reviewed papers highlighted features that automate or incentivize strong credential use. Systems like [13] and [20] offer built-in password generators to create unique, complex passwords, while [8] enhances this with a password strength checker to provide immediate feedback, guiding users toward secure choices.

By embedding these tools, password managers alleviate the burden of manually crafting strong passwords, encouraging adoption of better security habits without requiring extensive user expertise. This proactive design is essential to combating prevalent security risks like password reuse. While usability improvements are essential, innovative architectural designs further push the boundaries of security and convenience, as discussed in the following section.

4.3. Innovative Architectural Designs

4.3.1.Generative Approaches

Generative password managers shift away from storage-based models, enhancing security by creating passwords on demand. [6] proposes a state-less manager generating passwords using a master password and site-specific data, eliminating storage risks. [2] (HIPPO) and [25] (SPHINX) use DE-PAKE and OPRF, respectively, to compute passwords without storing them, offering robust protection against compromise.

Usability is also addressed in generative designs. [22] (Versipass) employs image cues for graphical passwords, aiding recall, while [9] (Amnesia) generates passwords bilaterally between a server and smartphone. [23] (MonoPass) regenerates passwords with metadata, and [24] (PassMan) uses fixed and variable parameters for site-specific passwords. These systems highlight the potential of generative methods to balance security and usability.

4.3.2.Distributed and Multi-Device Systems

Distributed architectures enhance security by dispersing trust across multiple entities. [9] (Amnesia) splits secrets between a server and smartphone, requiring cooperation for password generation. [10] (NoKey) distributes key shares across devices using Shamir's Secret Sharing, preventing single-device compromise. [25] (SPHINX) adapts to multi-device use, such as with a smartphone and browser, while [11] (SplitPass) splits passwords between a device and cloud assistant. These designs mitigate risks by ensuring no single point holds all necessary data.

4.3.3.Hardware Integration

Hardware-based solutions add physical security layers. [8] uses a USB key to store an RSA private key, requiring its presence for decryption. [7] (PUFPass) integrates PUFs into hardware, generating device-specific passwords that resist replication. These approaches leverage physical components to bolster security, offering protection against remote attacks and enhancing trust in the system.

4.4. Cryptographic Techniques and Protocols

4.4.1.Encryption and Key Management

Strong encryption underpins password manager security. Among the reviewed papers, 8 (32%) explicitly mentioned the use of AES or equivalent algorithms to safeguard credentials, and 4 papers (16%) detailed the use of key derivation functions such as PBKDF2 or Argon2d to strengthen encryption keys.

Systems like [13, 15-21] employ AES-256 or equivalent algorithms to safeguard credentials. Key derivation functions, such as PBKDF2 in [20] and [21], strengthen encryption keys derived from user passwords. Additionally, [6] employs Argon2d for key derivation, while [23] (MonoPass) uses PBKDF2 to strengthen encryption keys derived from the master password.

Innovative storage strategies further enhance protection. [13] splits encrypted data across multiple locations, while [16] (DFF-PM) uses a decentralized file format to distribute credentials, complicating unauthorized access. These methods ensure robust data security even under attack.

4.4.2.Privacy-Preserving Mechanisms

Privacy preservation is vital when managers are compromised. [2] (HIPPO) and [25] (SPHINX) use Oblivious Pseudo-Random Functions (OPRF) to generate passwords without exposing them to the manager, maintaining security post-breach. [12] integrates biometrics with privacy-preserving templates, protecting sensitive data even if the system is accessed. These mechanisms safeguard user privacy under adverse conditions.

4.4.3.Novel Protocols

Cryptographic innovation drives new security paradigms, and 12% of the reviewed papers introduced or utilized novel protocols to enhance password management security. As discussed in Section 4.1.1, HIPPO [2] uses DE-PAKE to generate passwords without storing them, which also underpins its novel cryptographic protocol, while [9] (Amnesia) employs a bilateral generation protocol between devices. SPHINX [25], as previously described in Section 4.1.1, employs OPRF to ensure privacy preservation even if the manager is compromised, contributing to its advanced protocol design.

5. Discussion

The analysis of 25 research papers on password managers reveals a dynamic landscape where security and usability are in constant tension. This discussion synthesizes the key findings, identifies overarching trends and divergent approaches, highlights gaps in the current research, compares the strengths and weaknesses of various solutions, and explores the implications for the future development of password management systems.

5.1. Synthesis of Findings

A central theme across the reviewed papers is the shift toward innovative designs that prioritize security without compromising usability. Furthermore, some researchers have explored unconventional methods to bolster security. For instance, Ahuja et al. [27] integrate steganography with encryption, hiding encrypted credentials within images to obscure their existence from potential attackers, representing a creative direction in password manager design. Several common trends emerge:

- Generative Approaches: A significant number of papers (28%) [2, 6, 9, 22-25] advocate for generative password managers that create passwords on demand rather than storing them. This eliminates the risk of vault compromise—a critical vulnerability in traditional systems. However, these approaches often require users to remember additional information, such as hints or metadata, which can introduce usability challenges.

- Distributed and Multi-Device Systems: Papers such as [9-11, 25], which present (16%) of the papers, emphasize the use of distributed architectures to avoid single points of failure. By splitting secrets or leveraging multiple devices, these systems enhance resilience against device compromise. Yet, they can introduce complexity in setup and usage, particularly when network connectivity is required.
- Hardware Integration: The incorporation of hardware components, such as USB keys [8] or Physically Unclonable Functions (PUFs) [7], adds an extra layer of security by tying credentials to physical devices. This approach was highlighted in 8% of papers. While this significantly enhances security, it may limit portability and convenience, as users must carry specific hardware.
- Usability Enhancements: Efforts to improve usability are evident in papers like [22], which uses image cues to aid password recall, and [3], which integrates directly with websites to streamline tasks. Biometric authentication, as explored in [17] and [12], offers a simplified access method but raises privacy concerns and requires fallback mechanisms.

Divergent approaches are also notable, particularly in the use of cloud-based versus local storage solutions. While cloud-based systems [13-15, 20] offer convenience and synchronization, they introduce potential attack vectors. In contrast, local or distributed systems [10, 11] prioritize security but may sacrifice ease of use. Another divergence lies in the reliance on master passwords: traditional systems use them to unlock vaults, whereas innovative designs like [10] eliminate them entirely, and [23] uses them solely for password generation.

5.2. Identification of Gaps

Despite the advancements, several gaps in the current research landscape warrant further exploration:

- Usability Testing: Many proposed systems, such as those in [22] and [23], lack comprehensive usability evaluations. Real-world testing with diverse user groups is essential to ensure that security innovations do not hinder adoption.
- Scalability of Distributed Systems: While distributed architectures enhance security, their scalability (particularly in scenarios with numerous devices or intermittent connectivity) remains underexplored. For instance, the scalability of NoKey's distributed system [10] remains untested in large-scale, real-world scenarios, where managing numerous devices could become impractical.
- Stronger Cryptographic Protocols: While password managers currently depend on well-established encryption methods like AES, future research could enhance their security by incorporating advanced cryptographic techniques. For example, exploring post-quantum cryptography could protect password managers from emerging threats posed by quantum computing, ensuring long-term security as quantum technologies evolve. Additionally, integrating methods like homomorphic encryption or secure multiparty computation could further improve security by enabling privacy-preserving computations and distributed trust models.
- Standardization and Interoperability: The diversity of approaches complicates user transitions between systems or devices. Developing common protocols or standards could enhance interoperability and user experience.

5.3. Comparison of Solutions

A comparison of the reviewed solutions reveals distinct strengths and weaknesses:

- Generative Approaches: Systems like [2] and [25] offer robust security by avoiding password storage but may impose a cognitive burden on users, who must remember additional inputs like hints or metadata.
- Distributed Systems: Solutions such as [9] and [10] provide resilience against device compromise but can be complex to set up and may require reliable network connectivity, limiting their practicality for some users.
- Hardware-Based Solutions: [8] and [7] deliver high security by binding credentials to physical devices, but at the cost of portability and convenience, as users must manage and carry specific hardware.
- Usability-Focused Designs: [3] prioritizes user-friendliness through direct website integration but may introduce new vulnerabilities if not carefully implemented. Similarly, biometric solutions ([17], [12]) simplify access but must address privacy and fallback concerns.

These comparisons underscore the trade-offs inherent in password manager design, where enhancing one aspect (e.g., security) often comes at the expense of another (e.g., usability).

5.4. Implications for Future Development

The findings from this review have several implications for the future of password management:

- Balancing Security and Usability: Future systems must continue to innovate in ways that do not overburden users. This could involve more intuitive interfaces, seamless multi-device synchronization, and educational features that help users understand security benefits.
- Hybrid Models: Combining generative and distributed approaches could offer a balanced solution,

leveraging the security of non-storage-based systems with the resilience of multi-device architectures.

- Biometric and Hardware Integration: While promising, these features should be optional or supplemented with alternative authentication methods to accommodate diverse user needs and contexts.
- Standardization Efforts: Industry-wide collaboration on protocols and standards could facilitate smoother user experiences and broader adoption, particularly as password managers evolve into more comprehensive identity management tools.

In conclusion, the reviewed papers collectively point toward a future where password managers are more secure, resilient, and user-centric. However, achieving this vision requires ongoing research to address usability gaps, scalability challenges, and the need for stronger cryptographic foundations. By learning from the strengths and weaknesses of current solutions, developers can create next-generation password managers that effectively balance security and convenience, ultimately fostering greater user adoption and trust.

6. Conclusion

This review of twenty-five research papers underscores the pivotal role password managers play in securing online accounts amidst the growing complexity of digital authentication. By synthesizing insights from diverse studies, this paper has explored advancements in addressing security challenges, enhancing usability, and pioneering innovative designs in password management.

The analysis reveals significant progress in tackling security vulnerabilities such as offline attacks, phishing, and device compromise. Generative systems, like those proposed in [6] and [25], eliminate password storage by creating credentials on demand, while distributed architectures, such as [10] and [11], enhance resilience by splitting secrets across multiple devices. Hardware-integrated solutions, including PUFs [7] and USB keys [8], add physical security layers, collectively reducing risks associated with traditional vault-based approaches. However, these innovations often introduce usability challenges. For instance, distributed systems may require network connectivity, and hardware-based designs can compromise portability, highlighting the persistent tension between security and user-friendliness.

Usability remains a critical determinant of adoption, with studies emphasizing the need for intuitive interfaces and simplified authentication. Innovations like biometric integration [12, 17] and user interface improvements [3, 22] demonstrate potential to reduce cognitive load and encourage secure practices. Yet, the review identifies gaps, such as insufficient real-world usability testing and the scalability of distributed systems, which limit the practical impact of these advancements.

For researchers and practitioners, the findings suggest a dual focus: prioritizing user-centric designs that balance security with accessibility and leveraging hybrid models that combine the strengths of generative, distributed, and hardware-based approaches. Standardization efforts could further enhance interoperability and user experience, fostering broader adoption.

Looking ahead, future research should explore comprehensive usability evaluations, scalable distributed architectures, and stronger cryptographic protocols to address evolving threats. By building on these insights, the next generation of password managers can better safeguard users while meeting the diverse needs of an increasingly digital world. These insights can guide developers in creating password managers that prioritize both security and user adoption, ultimately fostering a more secure digital ecosystem.

References

[1] A. Das, J. Bonneau, M. Caesar, N. Borisov, X. Wang, The tangled web of password reuse, In 21st Annual Network and Distributed System Security Symposium (NDSS) (2014) 23-26, https://doi.org/10.14722/ndss.2014.23357

[2] M. Shirvanian, C. R. Price, M. Jubur, N. Saxena, S. Jarecki, H. Krawczyk, A hidden-password online password manager, In 36th Annual ACM Symposium on Applied Computing (SAC '21) (2021) 1683-1687, https://doi.org/10.1145/3412841.3442131

[3] T. Safaie, ByPass: Reconsidering the usability of password managers, M.A.Sc. thesis, Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada, 2021

[4] F. Alodhyani, G. Theodorakopoulos, P. Reinecke, Password managers—It's all about trust and transparency, Future Internet 12(11) (2020) 189, https://doi.org/10.3390/fi12110189

[5] H. A. Saleh, Leveraging social engineering techniques for ethical purposes: An approach to develop fake Android app for collecting valuable data discreetly, Wasit Journal of Computer and Mathematics Science 3(3) (2024) 15-59, https://doi.org/10.31185/wjcms.268

[6] C. Rahalkar, D. Gujar, A secure password manager, International Journal of Computer Applications 178(44) (2019) 5-10, https://doi.org/10.5120/ijca2019919323

[7] Q. Guo, J. Ye, B. Li, Y. Hu, X. Li, Y. Lan, G. Zhang, PUFPass: A password management mechanism based on software/hardware codesign, Integration 64 (2019) 173-183, https://doi.org/10.1016/j.vlsi.2018.10.003

[8] Z. Petrov, R. Ragazan, Password manager with 3-step authentication system, In National Conference on Informatics, Dedicated to the 80th Anniversary of the Birth of Professor Peter Barnev (2016) 121-128

[9] L. Wang, Y. Li, K. Sun, Amnesia: A bilateral generative password manager, In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS) (2016) 313-324, https://doi.org/10.1109/ICDCS.2016.90

[10] F. Zinggeler, NoKey - A distributed password manager, M.S. thesis, ETH Zurich, Zurich, Switzerland, 2018

[11] Y. T. Liu, D. Du, Y. B. Xia, H. B. Chen, B. Y. Zang, Z. Liang, SplitPass: A mutually distrusting two-party password manager, Journal of Computer Science and Technology 33(1) (2018) 98-115, https://doi.org/10.1007/s11390-018-1810-y

[12] B. Yang, H. Chu, G. Li, S. Petrovic, C. Busch, Cloud password manager using privacy-preserved biometrics, In 2014 IEEE International Conference on Cloud Engineering (2014) 610-614, https://doi.org/10.1109/IC2E.2014.41

[13] Y. Kumarakalva, V. S. G. S., S. K. K., S. P. H., A. G. R., A secure password manager, Journal of Emerging Technologies and Innovative Research 4(03) (2017) 204-206, https://doi.org/10.51584/IJRIAS.2025.10040003

[14] K. Baskar, K. Muthumanickam, P. Vijayalakshmi, S. Kumarganesh, A strong password manager using multiple encryption techniques, Journal of the Institution of Engineers (India): Series B (2024) 1-8, https://doi.org/10.1007/s40031-024-01144-6

[15] M. Kanela, H. Dhingra, M. Singhal, G. Dhand, Secure and manage passwords with encryption and cloud storage, In 4th International Conference on Innovative Computing and Communication (ICICC) (2021) 1-4, https://doi.org/10.2139/ssrn.3833469

[16] S. Agholor, A. S. Sodiya, A. T. Akinwale, O. J. Adeniran, A secured mobile-based password manager, In 2016 IEEE Conference on Digital Information Processing and Communications (ICDIPC) (2016) 103-110, https://doi.org/10.1109/ICDIPC.2016.7470800

[17] H. A. Saleh, BANK OF PASSWORDS: A secure Android password manager implemented based on specific requirements, Al-Kitab Journal of Pure Science 8(1) (2024) 40-62, https://doi.org/10.32441/kjps.08.01.p5

[18] L. V. Cherckesova, O. A. Safaryan, O. S. Buryakova, V. M. Porksheyan, Development of password manager using cryptographic algorithms for data protection in Windows and Linux operating systems, Pakistan Journal of Life and Social Sciences 22(2) (2024) 20107-20115, https://doi.org/10.57239/PJLSS-2024-22.2.001472

[19] B. Englert, P. Shah, On the design and implementation of a secure online password vault, In 2009 International Conference on Convergence and Hybrid Information Technology (ICHIT'09) (2009) 375-382, https://doi.org/10.1145/1644993.1645063

[20] O. Hakbilen, P. Perinparajan, M. Eikeland, N. Ulltveit-Moe, SAFEPASS - Presenting a convenient, portable and secure password manager, In 4th International Conference on Information Systems Security and Privacy (ICISSP) (2018) 292-305, https://doi.org/10.5220/0006603102920303

[21] R. Zhao, C. Yue, Toward a secure and usable cloud-based password manager for web browsers, Computers & Security 46 (2014) 32-47, https://doi.org/10.1016/j.cose.2014.07.003

[22] E. Stobert, R. Biddle, A password manager that doesn't remember passwords, In 2014 New Security Paradigms Workshop (2014) 39-53, https://doi.org/10.1145/2683467.2683471

[23] H. Jeong, H. Jung, MonoPass: A password manager without master password authentication, In 26th International Conference on Intelligent User Interfaces Companion (IUI '21 Companion) (2021) 52-55, https://doi.org/10.1145/3397482.3450720

[24] J. B. Billa, M. M. H. Sbakil, A. Nawar, PassMan: A new approach of password generation and management without storing, In 7th International Conference on Smart Computing and Communications (ICSCC) (2019) 1-6, https://doi.org/10.1109/ICSCC.2019.8843591

[25] M. Shirvanian, S. Jarecki, H. Krawczyk, N. Saxena, SPHINX: A password store that perfectly hides passwords from itself, In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (2017) 1094-1105, https://doi.org/10.1109/ICDCS.2017.64

[26] H. Bojinov, E. Bursztein, X. Boyen, D. Boneh, Kamouflage: Loss-resistant password management, In 15th European Symposium on Research in Computer Security (ESORICS 2010) (2010) 286-302, https://doi.org/10.1007/978-3-642-15497-3_18

[27] R. Ahuja, M. Ramrakhyani, B. Manchundiya, S. Shroff, Dual layer secured password manager using Blowfish and LSB, International Journal of Computer Applications 143(3) (2016) 5-11, https://doi.org/10.5120/ijca2016910048

[28] H. S. Al-Sinani, C. J. Mitchell, Using CardSpace as a password manager, In Second IFIP WG 11.6 Working Conference on Policies and Research Management (IDMAN) (2010) 18-30, https://doi.org/10.1007/978-3-642-17303-5_2