SURVEY ON PASSWORD MANAGERS

Bimal Krishna k.s, Arun C.S, Arya R.K, Ananthakrishna P.K, Reeny Zakarias, Sanam E Anto

Bimal Krishna k.s student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Arun C.S student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Arya R.K student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

AnanthaKrishna P.K student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Reeny Zakarias Mentor, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Sanam E Anto Head of the Department, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

ABSTRACT

This paper examines the evolution and significance of password managers in enhancing digital security. Password managers are tools that store and generate complex, unique passwords for various accounts, minimizing the risks of weak or reused passwords. By utilizing encryption technologies, these applications ensure the protection of sensitive data, making it safer for users to manage their credentials. Additionally, password managers offer features such as autofill, synchronization across multiple devices, and breach monitoring, further improving convenience and security.The study evaluates a range of password manager applications, considering both open-source and proprietary options. It highlights the advantages of these tools, such as ease of use and robust protection against cyber threats, while also addressing their limitations and potential vulnerabilities. Issues like the risks of centralizing password storage and possible breaches are also discussed.User adoption of password managers is influenced by various factors, including ease of use, perceived security, and privacy concerns. As password managers become more prevalent, the paper also explores the future of passwordless authentication methods, which aim to eliminate the need for traditional passwords altogether.Overall, password managers play a critical role in the cybersecurity ecosystem, offering individuals and organizations a more secure, manageable way to handle online credentials. Their continued development and integration into broader security practices will likely shape the future of digital security and authentication.

Keyword: *- Password manager, encryption, cybersecurity, authentication, passwordless login, digital security.*

1. INTRODUCTION

With the exponential rise in online services, individuals are expected to create and remember multiple complex passwords. However, the human brain is not naturally suited for managing large numbers of unique credentials, which often leads to password reuse and weak security practices. This has given rise to the adoption of password managers—software tools designed to store and organize credentials in an encrypted vault. Password managers simplify digital security by generating strong passwords, storing them securely, and autofilling login credentials across websites and applications. This paper presents a comprehensive overview of the current landscape of password managers, their benefits, the challenges they face, and how they are poised to evolve in response to emerging cybersecurity threats and technological advancements.

2. MILESTONES

This section reviews research and developments in password manager technology. Studies have shown the effectiveness of password managers in reducing phishing attacks and password fatigue. Some notable tools analyzed include LastPass, Bitwarden, 1Password, Dashlane, and KeePass. Researchers have focused on user interface design, usability issues, and the secure implementation of encryption algorithms. Various studies have also highlighted the risks such as master password compromise, storage vulnerabilities, and browser integration flaws. A growing body of literature now investigates passwordless authentication methods like biometric logins and WebAuthn as alternatives to traditional password-based systems. Despite some concerns, password managers remain a trusted ally in digital security, especially when combined with multi-factor authentication (MFA).

The article titled "Guaranteed Output Delivery with More than 1/3 of Malicious Corruption for Client-Server MPC Protocols and Applications" by Alexey Golenkov, Yulia Myshko, Olga Nissenbaum, Alexander Renev (2024).This paper explores the challenging problem of secure multiparty computation (MPC) in environments where a significant number of parties (more than one-third) may be malicious. Traditional MPC systems often assume that fewer than one-third of participants can act dishonestly to maintain integrity. However, the authors propose an enhanced client-server model that ensures guaranteed output delivery—meaning honest clients always receive correct results—despite the high level of corruption. The paper contributes to cryptographic protocol development, with practical applications in secure voting, private financial computations, and collaborative data analysis, even in highly adversarial settings.

The article titled "Creating Computer Confidence: An Investigation into Current Privacy and Security Concerns of the Senior Demographic" by Caroline Hillier (2022).This study investigates how older adults perceive and handle online privacy and security, revealing that many in this demographic experience anxiety and lack confidence when using digital tools. The research highlights barriers such as unfamiliar terminology, fear of scams, and distrust in digital platforms, which hinder seniors' participation in the digital world. By understanding these concerns, the paper aims to inform the design of more intuitive interfaces, educational programs, and support systems that empower seniors to safely and confidently use technolog

The article titled "MonoPass: A Password Manager without Master Password Authentication" by Hyeonhak Jeong, Hyunggu Jung (2021).MonoPass presents a fresh take on password management by eliminating the need for a master password, which is often a single point of failure in traditional password managers. Instead, it uses alternative forms of authentication, such as biometric or device-based verification, to maintain security while improving usability. This approach addresses common security flaws like password reuse or forgetting the master password, offering a more seamless and secure experience for users. The paper also evaluates MonoPass in real-world use cases, demonstrating its potential to replace conventional systems.

The article titled "Password Manager with Multi-Factor Authentication" by R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan, Saleem Basha (2023).This paper proposes a password management system that integrates multi-factor authentication (MFA) to significantly enhance security. The authors design a system that combines traditional password storage with additional layers of verification, such as biometrics (e.g., fingerprint recognition), one-time passwords (OTPs), and email verification. This layered approach mitigates risks associated with password theft and unauthorized access. The paper emphasizes the need for such systems in an era of increasing cyber threats, especially in contexts like e-banking and cloud services.

The article titled "Performance analysis and survey on security of password managers and various schemes of P2P models" by Aditya Kamat, Chitrarth Tomar, Abhishek Tainwala, Syed Akram (2018).This paper provides a comprehensive survey and performance analysis of various password managers, focusing on their architecture, encryption methods, and user security. The authors also delve into peer-to-peer (P2P) models that allow decentralized password sharing and storage, examining their potential to improve scalability and eliminate central points of failure. The paper evaluates the trade-offs between security, speed, and usability, offering insights into how different password managers perform under various conditions and suggesting improvements to current systems.

This research applies Zipf's Law—a principle where a few items occur very frequently while most occur rarely—to analyze user-generated passwords. The authors demonstrate that human password choices often follow this predictable distribution, which makes common passwords highly vulnerable to guessing attacks. By understanding these statistical patterns, the paper informs both attackers (in creating better cracking tools) and defenders (in enforcing stronger password policies). The study contributes to the ongoing debate about balancing password complexity, memorability, and security.

This paper explores the concept of "usable security," which refers to designing secure systems that are also easy and intuitive for users. The authors argue that many security tools fail because they are too complex or burdensome, causing users to bypass them. Through qualitative research and case studies, they analyze how users perceive and interact with security mechanisms, identifying key factors such as trust, accessibility, and simplicity. The study advocates for a user-centered approach to cybersecurity design, emphasizing that the best security solutions are the ones people will actually use correctly.

This paper introduces a hardware-based password management solution where encrypted credentials are stored on a USB pen drive. To access online accounts, users must plug in the device, which adds a layer of physical security. The system eliminates the need to remember multiple passwords and ensures that data is protected even if the main device is compromised. The authors also discuss encryption techniques, user interface design, and the advantages of portable security devices in managing digital identities, particularly in offline or low-trust environments.

A milestone for the paper "That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers" by Sean Oesch and Scott Ruoti involves a detailed review of the study to understand the current security posture of browser-based password managers. The paper evaluates how major browsers handle password generation, secure storage, and autofill features, identifying both improvements and persisting vulnerabilities since previous evaluations. The milestone includes analyzing the methodology used in the study, such as threat modeling and real-world attack scenarios, to assess the reliability and relevance of the findings. Special attention is given to the autofill functionality, which the paper highlights as a significant security concern, especially when interacting with malicious or compromised websites. The goal is to extract meaningful insights from the study that can help in the design, development, or assessment of secure password management solutions. This includes understanding best practices, potential attack vectors, and the authors' proposed recommendations for strengthening password manager security. Completing this milestone will contribute to a broader understanding of secure user authentication practices and inform future work in the field of cybersecurity, particularly in developing safer, more resilient browser-based password managers.

A milestone for the paper "Choosing the Right Password Manager" by Elizabeth A. Gallagher (Serials Review, 2019) involves reviewing the article to understand how users can evaluate and select a suitable password manager based on usability, security, and functionality. The milestone focuses on identifying key criteria presented in the paper that influence user decisions, such as ease of use, compatibility across devices, encryption standards, and the presence of additional features like autofill, password generation, and secure sharing. The paper also discusses the balance between convenience and security, offering guidance on what users should prioritize when selecting a password manager. Through this milestone, the goal is to summarize the strengths and limitations of various password manager options presented, and to analyze how well these tools align with user needs and security best practices. This understanding can be applied to either personal use or for making recommendations in institutional settings such as libraries or IT departments. By completing this milestone, one can develop a more informed perspective on the criteria that make a password manager effective and trustworthy, which is valuable when guiding users or stakeholders in selecting secure digital identity management solutions.

A milestone for the paper "Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers" by Ramakrishna Ayyagari, Jaejoo Lim, and Olger Hoxha (Contemporary Management Research, 2019) involves analyzing the psychological and behavioral factors that influence users' reluctance or intention to adopt password managers. This study uses a research model grounded in behavioral theories to explore perceptions such as ease of use, perceived usefulness, security concerns, and trust, as well as the role of social influence and user awareness. The milestone includes reviewing the methodology used in the study, such as survey data and statistical analysis, to understand how these variables affect adoption behavior. The goal is to extract insights into the barriers preventing widespread use of password managers despite their known benefits, and to identify strategies that could promote their adoption. This milestone is valuable for those involved in cybersecurity education, product development, or user experience design, as it provides evidence-based reasons behind user hesitancy. Understanding these motivations can help in designing more user-friendly password management solutions, crafting targeted awareness campaigns, or enhancing trust through better security transparency and support. Completing this milestone contributes to both academic understanding and practical improvements in user security behavior.

A milestone for the paper "Why Do People Adopt, or Reject, Smartphone Password Managers?" by Nora Alkaldi and Karen Renaud (2016) involves examining the factors that influence user decisions to either use or avoid password managers on smartphones. This study investigates the psychological, social, and usability-related aspects that shape adoption behaviors, particularly in the context of mobile technology. The authors explore issues such as trust, perceived usefulness, ease of use, and fear of data breaches, as well as the influence of habits and previous experiences with security tools. The milestone includes reviewing the qualitative research methods used, such as interviews and surveys, to understand how user perceptions are formed and what motivates or discourages the use of password managers on mobile devices. The goal is to gain insight into the human-centric challenges of promoting password manager adoption, especially in a mobile-first world. This knowledge is useful for developers, UX designers, and cybersecurity educators aiming to improve user trust and engagement. By completing this milestone, one can better understand the personal and contextual reasons behind adoption or rejection, and apply these insights to design more intuitive, secure, and appealing mobile password management solutions that align with user expectations and behaviors.

A milestone for the paper "The Emperor's New Autofill Framework: A Security Analysis of Autofill on iOS and Android" by Sean Oesch, Anuj Gautam, and Scott Ruoti (arXiv preprint, 2021) involves studying the security implications of autofill frameworks used in mobile operating systems, specifically iOS and Android. This milestone focuses on understanding how autofill services function on these platforms, the potential vulnerabilities they introduce, and how malicious applications might exploit these weaknesses to steal sensitive user data, such as credentials or personal information. The authors conduct a comprehensive security analysis by examining the underlying mechanisms of autofill APIs and testing real-world applications to uncover inconsistencies and flaws in how autofill is triggered and handled. The goal of this milestone is to summarize the key findings from the paper, evaluate the risks associated with mobile autofill, and understand the authors' recommendations for improving platform security. This information is critical for mobile developers, security researchers, and policy-makers who aim to ensure safe and secure user experiences. By completing this milestone, one can gain valuable insight into mobile autofill threats and defenses, which can inform the design of safer mobile apps and guide users in making secure choices when relying on autofill services.

A milestone for the paper "The Tangled Web of Password Reuse" by Anupam Das et al. (NDSS, 2014) involves analyzing the patterns, risks, and implications of password reuse across different online platforms. This study investigates how users tend to reuse or slightly modify their passwords across services, which significantly increases the risk of credential-stuffing attacks and compromises overall account security. The milestone includes reviewing the authors’ methodology, which involves data analysis from real-world password leaks to uncover trends in reuse behaviors and common password transformation patterns. The goal is to understand how attackers can exploit these patterns using automated tools, and why password reuse remains a persistent security problem despite awareness efforts. By completing this milestone, one should be able to summarize the key findings and draw conclusions about user behavior, security risks, and potential mitigation strategies. This includes exploring the role of password managers and education in reducing reuse. The insights gained can support efforts in designing systems that detect or discourage password reuse, developing more secure authentication mechanisms, or raising user awareness. Ultimately, this milestone helps highlight the critical importance of unique and strong passwords in personal and organizational cybersecurity.

A milestone for the paper "A Usability Study and Critique of Two Password Managers" by Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle (USENIX Security Symposium, 2015) involves analyzing the usability aspects of two popular password managers, identifying both strengths and weaknesses in terms of user experience. The study evaluates the effectiveness, ease of use, and security of these password managers by conducting user studies where participants interact with the tools in real-world scenarios. The milestone includes reviewing the paper’s methodology, which involves assessing how well users can manage their passwords using the software, how easily they understand its features, and how secure they feel during usage. Key insights include identifying usability barriers that may discourage users from fully adopting password managers, such as complexity in setup, lack of clear instructions, or poor integration with browsers and apps. The goal of this milestone is to summarize the usability critiques and suggest potential improvements for making password managers more user-friendly, while still maintaining strong security. By completing this milestone, one will gain a better understanding of the challenges users face when using password management tools, which can inform future designs of more intuitive and accessible password management solutions that encourage widespread adoption.

In their 2006 paper "A Usability Study and Critique of Two Password Managers," Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle conducted one of the earliest and most influential empirical studies assessing the usability of password management tools. Their work marked a significant milestone in the intersection of usability and security, highlighting how security tools often fail due to poor user-centered design. The study involved real users interacting with two widely available password managers, analyzing their behavior, usability challenges, and attitudes toward the tools. The researchers uncovered critical issues, such as users' confusion around password storage, lack of trust in automation, and difficulties with the user interface. They emphasized that security mechanisms must be intuitive and accessible to end-users to be effective. This work not only laid the groundwork for future usability studies in security software but also influenced the design philosophy of later password managers by stressing the importance of human-centric design and testing.

The 2015 paper "Cracking-resistant password vaults using natural language encoders" by Rahul Chatterjee et al. presents a significant advancement in the security of password management systems. The authors introduced a novel approach to constructing password vaults that are more resistant to offline cracking attacks. Their system, called "NLP-PP," uses natural language processing (NLP) techniques to encode vault secrets into natural language-like structures, making brute-force attacks significantly harder for adversaries. This innovation addressed a critical weakness in traditional password vaults, which often rely solely on encryption tied to a master password and are vulnerable if that password is weak. By leveraging syntactic patterns from natural language, the authors increased the entropy of the stored data while maintaining usability. This work is a milestone in password management research, as it was one of the first to apply NLP in the context of secure password storage and influenced later approaches to creating more robust and user-friendly vault systems.

The 2010 paper "A Comparative Usability Evaluation of Traditional Password Managers" by Ambarish Karole, Nitesh Saxena, and Nicolas Christin marks a critical step forward in understanding how different password managers perform in real-world usability scenarios. The study systematically evaluated multiple password managers—including both web-based and standalone applications—by observing how users interacted with them across common tasks. Through user studies, the authors identified key usability issues such as inconsistent user interfaces, confusion around auto-fill features, and challenges with password generation and retrieval. One of the major contributions of this work was the development of a usability framework specifically tailored to evaluate password managers. The paper also emphasized that usability flaws could significantly compromise security, as users may adopt insecure workarounds. This research served as a milestone by highlighting the importance of designing password managers that balance security with user experience, and it laid the groundwork for future usability-centric improvements in authentication tools.

The 2014 paper "Password Managers: Attacks and Defenses" by David Silver et al. represents a pivotal contribution to the security analysis of password management tools. This study systematically explored the attack surface of popular browser-based password managers, identifying a range of vulnerabilities such as auto-fill exploits, insecure storage mechanisms, and poor handling of malicious iframes. The authors presented detailed threat models and demonstrated real-world attack scenarios that compromised stored credentials without user interaction. Importantly, the paper didn't just focus on exposing flaws—it also proposed concrete defense mechanisms and best practices for both users and developers. By highlighting the gap between user convenience and security implementation, the research helped shift attention toward more secure and resilient password manager design. This work stands as a milestone for its comprehensive security evaluation, raising awareness among both the academic community and industry stakeholders, and influencing the design of more secure password management features in modern browsers.

The article titled “Security Now! by Steve Gibson”, released in 2015, serves as a notable milestone in public cybersecurity education, particularly regarding password management and security practices. In this episode, Gibson discussed key vulnerabilities in password managers, browser-based auto-fill features, and the implications of poor design choices on user security. His analysis, while informal compared to academic research, was technically thorough and accessible to a broad audience. Gibson also emphasized the importance of zero-knowledge architecture, strong encryption, and user awareness in maintaining secure password storage. What sets this work apart is its role in bridging the gap between complex security topics and the general public. By providing clear, actionable advice and dissecting real-world threats, this episode contributed to raising awareness about the risks of relying on insecure password practices. It stands as a milestone for its influence on both technically savvy listeners and everyday users seeking to understand and improve their digital security posture.

The 2009 paper "Improving Multiple-Password Recall: An Empirical Study" by J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer is a foundational contribution to understanding human memory limitations in password management. The study focused on the growing challenge users face in remembering multiple strong passwords and explored strategies to improve password recall without compromising security. Through a controlled empirical study, the authors examined techniques such as mnemonic devices, password grouping, and contextual cues to enhance users' ability to remember numerous passwords over time. One of the key findings was that password recall could be significantly improved by aligning password creation and usage with cognitive principles. This work stands as a milestone because it addressed a critical usability problem in authentication—how users interact with multiple credentials in real-world settings. It helped shape future research in user-centered security and inspired the design of tools and practices aimed at making secure password use more manageable and intuitive.

The 2013 paper "Honeywords: Making Password-Cracking Detectable" by Ari Juels and Ronald L. Rivest represents a groundbreaking advancement in password security. The authors introduced the concept of "honeywords" — decoy passwords stored alongside real ones in authentication systems. If an attacker compromises the password file and attempts to use a honeyword, the system can detect the intrusion and trigger alerts or protective measures. This approach shifts the security paradigm from solely preventing breaches to enabling detection of unauthorized access attempts. A key advantage of honeywords is that they can be implemented with minimal disruption to existing authentication systems while significantly increasing security awareness. The proposal addressed a longstanding issue: the silent failure of systems once password hashes are leaked. As a milestone, this work not only introduced an innovative defense mechanism but also influenced a new line of research focused on intrusion detection and proactive response in authentication systems.

S. Agholor’s 2015 paper, "The Use of Screen Lock Options in Securing Mobile Phones," published in the Akoka Journal of Vocational and Science Education, provides a critical examination of user behavior and the effectiveness of various screen lock mechanisms on mobile devices. The study analyzed common screen lock methods—such as PINs, passwords, patterns, and biometric options—and assessed their adoption rates and perceived security among mobile users. Agholor highlighted the gap between available security features and actual user practices, showing that convenience often outweighs security in user decisions. The paper contributed to understanding how users balance usability and protection, particularly in mobile contexts where device loss or theft is common. As a milestone, this research emphasized the importance of user education and intuitive security design, encouraging further exploration into enhancing mobile security without compromising ease of access. It laid the groundwork for future studies on mobile authentication and informed developers about user-centric security considerations.

The 2009 paper "Password Cracking Using Probabilistic Context-Free Grammars" by M. Weir, S. Aggarwal, B. Glodek, and B. de Medeiros marked a major breakthrough in the field of password security and attack modeling. The authors introduced a novel approach to password cracking by applying probabilistic context-free grammars (PCFGs) to model and predict human password creation patterns. Unlike brute-force or dictionary attacks, the PCFG method leverages the structure of passwords—such as common substitutions, capitalization patterns, and character sequences—to generate highly probable password guesses. This approach demonstrated a significant improvement in cracking efficiency, especially against real-world password datasets, as it could prioritize more likely passwords over less probable ones. The paper’s contribution is a milestone because it fundamentally changed how researchers and security professionals understand password vulnerabilities. It provided concrete evidence that human-generated passwords follow predictable patterns, and thus, are more vulnerable than previously assumed. The work spurred further research into both password strength analysis and the development of countermeasures like stronger password policies and user education.

The 2011 study "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms" by P. G. Kelly, S. Komanduri, M. L. Mazurek, R. Shay, T. V. Lujo, B. N. Christin, et al., from Carnegie Mellon University, represents a key milestone in evaluating password security through realistic attack simulations. The authors advanced the field by developing a framework that simulates sophisticated password-cracking algorithms to assess the true strength of passwords, rather than relying solely on theoretical models or entropy-based metrics. Using large real-world datasets and modeling techniques like Markov chains and probabilistic algorithms, they demonstrated that commonly used password strength indicators often overestimate protection levels. This paper’s approach offered a more accurate and empirical method of measuring password strength, providing valuable insights for system administrators, researchers, and policy-makers. It marked a shift in password research from abstract complexity rules to data-driven assessments, influencing the design of better password meters and more informed password policy guidelines aimed at both usability and security.

3. CONCLUSIONS

Password managers provide a practical solution to the long-standing issue of password management. By offering secure storage, password generation, and autofill capabilities, they reduce the cognitive load on users and significantly improve security posture. As digital threats continue to evolve, password managers are also adapting by incorporating zero-knowledge encryption, biometric access, and integration with enterprise identity platforms. Looking forward, these tools will likely play a vital role in the transition to passwordless authentication methods, solidifying their importance in the future of cybersecurity.

4. REFERENCES

[1]. Guaranteed Output Delivery with More than 1/3 of Malicious Corruption for Client-Server MPC Protocols and Applications.Alexey Golenkov, Yulia Myshko, Olga Nissenbaum, Alexander Renev October 16, 2024.

[2]. Creating Computer Confidence: An Investigation into Current Privacy and Security Concerns of the Senior Demographic.,Caroline Hillier (2022)

[3]. MonoPass: A Password Manager without Master Password Authentication,Hyeonhak Jeong, Hyunggu Jung April 2021.

[4]. Password Manager with Multi-Factor Authentication,R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan, Saleem Basha April 2023.

[5]. Performance analysis and survey on security of password managers and various schemes of P2P models Aditya Kamat, Chitrarth Tomar, Abhishek Tainwala, Syed Akram May 18 (2018)

[6]. The Use of Screen Lock Options in Securing Mobile Phones Agholor, S. (2015).

[7]. Why Do People Adopt, or Reject, Smartphone Password Managers Alkaldi, N., & Renaud, K. July 18, 2016

[8]. A Study on the Intention to Use Password Managers Ayyagari, R., Lim, J., & Hoxha, O. December (2019)

[9]. Cracking-resistant password vaults using natural language encoders.,Chatterjee, R., et al. July 2015

[10]. A Usability Study and Critique of Two Password Managers.,Chiasson, S., van Oorschot, P. C., & Biddle, R. July 31, 2006

[11]. The Tangled Web of Password Reuse.,Das, A., et al. February 23 (2014).

[12]. Choosing the Right Password Manager.,Gallagher, E. A. (2019).

[13]. Honeywords: Making Password-Cracking Detectable.,Juels, A., & Rivest, R. L. November 2013.

[14]. A Comparative Usability Evaluation of Traditional Password Managers.,Karole, A., Saxena, N., & Christin, N. December 2010

[15]. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms,Kelly, P. G., et al May 23, 2012.

[16]. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers,Oesch, S., & Ruoti, S. August 14, 2020

[17]. The Emperor's New Autofill Framework: A Security Analysis of Autofill on iOS and Android,Oesch, S., Gautam, A., & Ruoti, S. December 10, 2021

[18]. Password Managers: Attacks and Defenses,Silver, D., et al. August 22, 2014

[19]. Password Cracking Using Probabilistic Context-Free Grammars,Weir, M., Aggarwal, S., Glodek, B., & de Medeiros, B. May 2009

[20]. *Improving Multiple-Password Recall: An Empirical Study*,Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. April 2009

[21]Security Now*!* is a weekly show hosted by Steve Gibson and Leo Laporte, focusing on computer security topics 2015

[22]. Zipf's Law in Passwords,Ding Wang, Gaopeng Jian, Xinyi Huang, and Ping Wang August 21, 2014

[23]. Exploring the Meaning of "Usable Security "Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg July 2020

[24] Pen-Drive Based Password Management System for Online Accounts,Samruddhi Patil, Kumud Wasnik, and Sudhir Bagade February 25, 2018,

[25] Analysis on the Security and Use of Password Managers",Carlos Luevanos, John Elizarraras, Khai Hirschi, Jyh-Haw Yeh 2017