PASSWORD GENERATOR AND MANAGER

RAAGHASHREE M
SRM institute of science and technology
Chennai,India
rm6984@srmist.edu.in

ARUL LINCY A
SRM institute of science and technology
Chennai,India
aa5192@srmist.edu.in

GAYATHRISRI G
SRM institute of science and technology
Chennai,India
gg6825@srmist.edu.in

***Abstract*— In place of conventional password managers, this study explores the world of password generators—systems created to generate unique passwords for websites on the fly. Numerous password generation techniques have been put forth and discussed in the literature over the previous fifteen years. But there hasn't been a generic model for these systems yet. In order to close this gap, the first thorough model for password generators is presented in this study. An objective and high-level evaluation of the design of such systems is based on the model. This paper seeks to contribute to the existing body of knowledge by providing a comprehensive exploration of contemporary password manager and generator systems to enable a more systematic evaluation of password generator designs by creating a unified model. In addition to facilitating a structured evaluation, the suggested model played a key role in the ideation of the innovative Auto Pass password generator system.**

Keywords—Password Manager, Generator, Master Password

I. INTRODUCTION

In an era dominated by digitalization and pervasive online activities, the paramount importance of robust cybersecurity practices cannot be overstated. Among the fundamental aspects of safeguarding digital assets, the creation and management of secure passwords stand as a linchpin in the defense against unauthorized access. Passwords, being the primary gatekeepers to our digital lives, necessitate careful consideration in their formulation and storage to thwart the ever-evolving landscape of cyber threats. Despite widespread skepticism over the degree of security they offer, secret passwords are nevertheless a fairly popular way to authenticate users. Passwords may still be used in the future, although there are a number of potentially useful technologies that could replace them, such as the usage of biometrics and trusted personal devices. Finding solutions to make pass-words easier to use and manage is still a critical issue for real-world security, given their widespread use now and their likely usage for the foreseeable future.

Users are clearly forced to compromise their own security when they are expected to memorize numerous strong passwords just to conduct their daily business on the Internet. The project's objective is to create a secure password management system that will let users create and store trustworthy passwords. The program will employ encryption methods to stop passwords and other private data from being lost or misused. It will have additional features, such as password generators, to provide users with a simple and effective experience.

II. BACKGROUND

The increasing amount of online accounts and services that people and businesses use has made password management a crucial component of digital security in recent years. There is a serious security risk associated with using weak passwords or using the same password for several accounts. These practices can result in financial losses and data breaches. It is not practical to remember all of the numerous accounts that the typical internet user has, each with its own set of login credentials. By giving users a safe way to store and manage their passwords, password management tools aim to solve this problem. With the help of these tools, users can create secure passwords, keep them safe in an encrypted vault, and have them ready to go when needed. By doing away with the need for users to memorize numerous passwords, this method lowers the possibility that they will use weak or similar passwords.

These days, using digital devices in our daily lives is essential. These devices are used for both personal and business needs, and they are now essential resources for anything from communication to amusement. On the other hand, there is an increased risk of identity theft, data breaches, and cyberattacks with increased use of these devices.

The importance of using secure password management systems to address this issue has increased. By using these tools, users can reduce the possibility that one of their accounts will be compromised by creating and remembering safe, unique passwords for every account. While there are many password management tools out there, not all of them are created equal. It is essential to choose one that uses industry-standard encryption techniques and security features to protect passwords and other sensitive data.

II. LITERATURE REVIEW

In the ever-evolving landscape of cybersecurity, the design and implementation of effective password generators and managers have garnered considerable attention from researchers, practitioners, and security enthusiasts. Password management systems have developed historically in response to the increasing intricacy of online activities and the need to improve security. Basic hashing and encryption methods were used by early password systems, but as cyber threats grew more advanced, researchers began looking into new strategies. In the literature piece, *Password Generators,* the majority of the literature is devoted to methods for creating passwords. Random string generators were suggested in early research, but there were issues with these passwords' memorability. Algorithms for creating secure and memorable passwords were developed as a result of further research into the psychology of password creation. These algorithms frequently make use of a mix of numbers, symbols, and capital and lowercase letters.

In *Usability and User Experience,* usability has been a critical consideration in the development of password generators and managers. Several studies explore the trade-off between security and user convenience. Balancing the creation of strong, complex passwords with user-friendly interfaces is an ongoing challenge, and the literature offers insights into effective design principles and user-centric approaches.

In the piece, *Biometric Integration* it is seen that recent advancements have witnessed the integration of biometric authentication into password management systems. Researchers explore the feasibility and security implications of combining traditional passwords with biometric identifiers. The promise of enhanced security through biometric data introduces new dimensions to the evolving landscape of password protection. Numerous case studies and comparative analyses populate the literature, offering critical evaluations of existing password generators and managers. Researchers dissect the strengths and weaknesses of popular solutions, providing insights into their efficacy in real-world scenarios. These analyses contribute to the ongoing discourse on refining and enhancing password security measures. The ever-evolving threat landscape necessitates adaptive security measures. The literature explores the integration of machine learning and artificial intelligence into password security. Adaptive systems that analyze user behavior, detect anomalies, and dynamically adjust security measures showcase the innovative strides taken to thwart emerging threats effectively.

The way passwords are managed and stored has undergone a paradigm shift with the introduction of cloud computing. Although cloud-based solutions provide advantages in terms of accessibility and synchronization, worries regarding the security of remotely stored passwords continue to exist. The current discourse revolves around encryption techniques and secure protocols, which reflects the continuous endeavor to balance the ease of remote storage with strong security precautions.

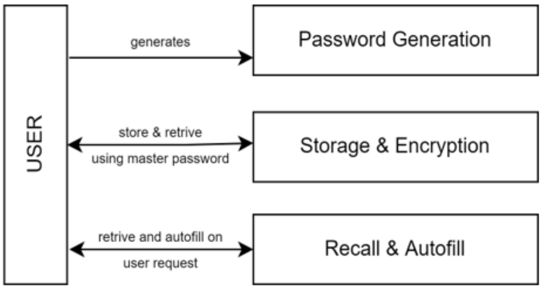
IV. METHODOLOGY

A. Database Design

In the realm of simple password management, the foundation lies in a well-structured database designed to securely store and organize sensitive user credentials. At its core, this database comprises tables, with a primary table housing key elements such as unique identifiers, usernames, and encrypted or hashed passwords. Each entry typically includes additional details like the associated website or application, user notes, and a categorization to facilitate organization. A fundamental security measure involves the encryption or hashing of passwords before storage, safeguarding sensitive information from potential breaches. Importantly, access to this repository is guarded by a master password, serving as the linchpin for unlocking and securing the stored credentials.

B.*Conceptual Design*

The conceptual design phase of a password manager and generator is a pivotal stage in the development process, shaping the core architecture, functionalities, and user interactions that define the essence of the system. At its core, this design prioritizes a user-centric approach, ensuring that the system is not only secure but also intuitive and seamlessly navigable for users. A key consideration lies in the secure storage architecture, encompassing database structure, encryption methodologies, and storage protocols to safeguard user credentials against unauthorized access. The conceptual design emphasizes secure login protocols and session management, and it includes user authentication and authorization mechanisms as essential elements. The value of an intuitive user interface (UI) cannot be emphasized, so in order to create an interface that is both aesthetically pleasing and functionally efficient, the conceptual design takes accessibility features, navigation flow, and visual elements into consideration.



General working of a password manager

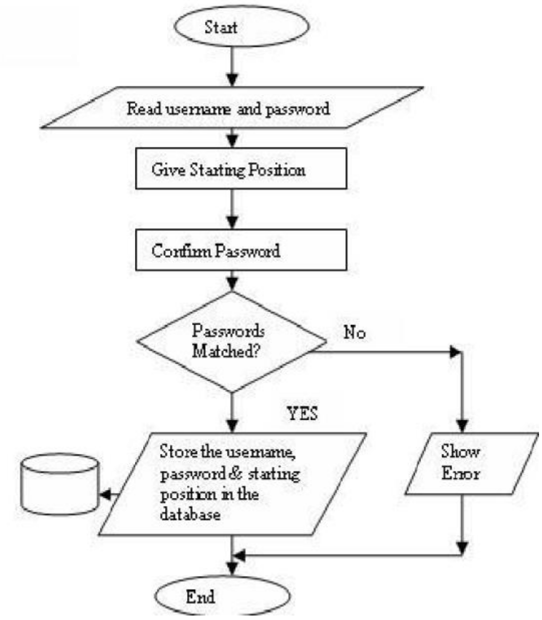
C. Architecture Design

The architecture design of a password manager and generator is a pivotal aspect of developing a secure, efficient, and user-friendly system. This phase delves into the underlying structure, components, and interactions that collectively form the foundation for a robust password management solution. The architecture begins with the design of the database structure, which serves as the repository for securely storing user credentials. A well-architected database typically comprises tables for usernames, encrypted passwords, associated websites or applications, and additional metadata. The choice of database technology and the ample mentation of secure storage protocols are critical considerations in safeguarding sensitive information. It incorporates advanced password generation algorithms that strike a balance between complexity and memorability. Randomness, character diversity, and adaptability to different security requirements are key considerations. The system should dynamically generate strong, unique passwords based on user-defined criteria.

.

D. Module design

Module design is a crucial phase in developing a simple password manager, as it delineates the system into discrete, manageable components, each with a specific set of functions. One key module is the User Interface (UI), which governs the visual and interactive aspects of the password manager. The UI module ensures a seamless user experience, facilitating tasks such as adding or updating passwords. Another critical module is the Password Generator, responsible for creating strong and unique passwords based on user preferences. The Encryption Module is fundamental to the security of stored credentials, employing robust algorithms to encrypt and protect sensitive data. The Database Module manages the storage and retrieval of password information, incorporating functionalities for data organization and retrieval efficiency. Additionally, the Authentication and Authorization Module verifies user identity and permissions, enhancing overall system security. These modular components work in concert to create a cohesive and efficient simple password manager, offering both security and user-friendly functionality.


Start
Read username and password
Give Starting Position
Confirm Password
Passwords Matched?
No
YES
Store the username, password & starting position in the database
Show Error
End

V .*Interface*

The user interface of the password manager offers a seamless and intuitive experience. With a clean design, the application presents a user-friendly layout, featuring input fields for customization and a clear display of generated passwords. The inclusion of options for password length and complexity ensures adaptability to individual preferences. Interactive buttons for password generation and copy-to-clipboard functionality enhance user convenience. Error handling is integrated for a smooth experience, making the application an accessible tool for creating secure and tailored passwords with ease.

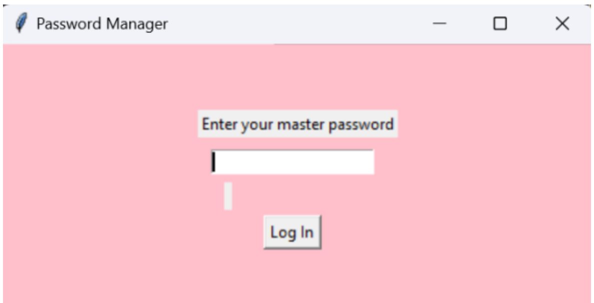
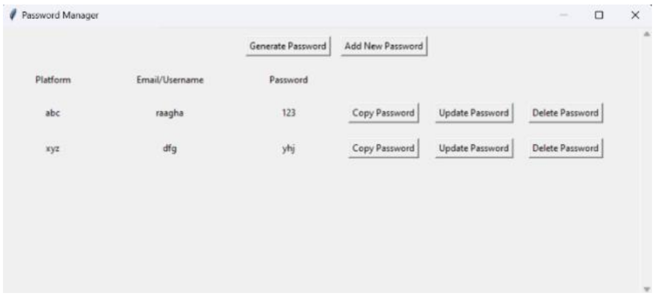
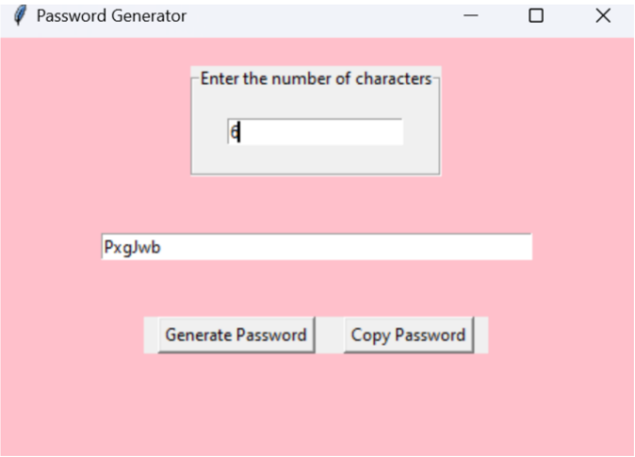


Figure I : Login page



Platform	Email/Username	Password			
abc	raagha	123	Copy Password	Update Password	Delete Password
xyz	dfg	yhj	Copy Password	Update Password	Delete Password

Figure II: Password Manager



6

PxgJwb

Figure III: Password Generator

CONCLUSION

Developing a password management system is an essential part of modern cybersecurity. This project is meant for individuals who use the internet frequently, create multiple online accounts, and struggle to remember all of the login details for their accounts because of the growing number of accounts and the complexity of passwords. Additionally, users are more likely to be the target of hacking attempts because of the increased risk associated with using weak passwords or the same password for multiple accounts. The use of a password management program can help lower these risks by providing users with a convenient and safe way to store and manage their passwords. All things considered, implementing a password management tool is an essential first step in improving online security and reducing the risks associated with using default or weak passwords. With the integration of cutting-edge technology and best practices, this solution can provide users with a safer and more efficient way to manage their passwords.

REFERENCES

[1] C. Herley and P. C. van Oorschot, “A research agenda acknowledging the persistence of passwords,” IEEE Security & Privacy, vol. 10, no. 1, pp. 28–36, 2012.

[2] D. Florencio, C. Herley, and P. C. van Oorschot, “Password portfolios ˆ and the finite-effort user: Sustainably managing large numbers of accounts,” in Proc. 23rd USENIX Security Symposium. USENIX Association, 2014, pp. 575–590.

[3] J. A. Halderman, B. Waters, and E. W. Felten, “A convenient method for securely managing passwords,” in Proc. WWW 2005, A. Ellis and T. Hagino, Eds. ACM, 2005, pp. 471–479.

[4] A. H. Karp, “Site-specific passwords,” HP Laboratories, Palo Alto, Tech. Rep. HPL-2002-39 (R.1), May 2003.

[5] M. Mannan and P. C. van Oorschot, “Passwords for both mobile and desktop computers: ObPwd for Firefox and Android,” USENIX ;login, vol. 37, no. 4, pp. 28–37, August 2012.

[6] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, “Stronger password authentication using browser extensions,” in Proc. 14th USENIX Security Symposium, P. McDaniel, Ed. USENIX Association, 2005, pp. 17–32.

[7] R. Wolf and M. Schneider, “The passwordsitter,” Fraunhofer Institute for Secure Information Technology (SIT), Tech. Rep., May 2006.

[8] K.-P. Yee and K. Sitaker, “Passpet: Convenient password management and phishing protection,” in Proc. SOUPS 2006, L. F. Cranor, Ed. ACM, 2006, pp. 32–43.

[9] F. A. Maqbali and C. J. Mitchell, “Password generators: Old ideas and new,” in Proc. WISTP 2016, ser. LNCS, S. Foresti and J. Lopez, Eds., vol. 9895. Springer, 2016, pp. 245–253.

[10] D. McCarney, “Password managers: Comparative evaluation, design, implementation and empirical analysis,” Master’s thesis, Carleton University, August 2013, available at https://danielmccarney.ca/assets/pubs/ McCarney.MCS.Archive.pdf.

[11] R. Biddle, M. Mannan, P. C. van Oorschot, and T. Whalen, “User study, analysis, and usable security of passwords based on digital objects,” IEEE Trans. Inf. Forensics & Security, vol. 6, no. 3, pp. 970–979, 2011.

[12] M. Mannan and P. C. van Oorschot, “Digital objects as passwords,” in Proc. HotSec’08, N. Provos, Ed. USENIX Association, 2008.

[13] M. Mannan, T. Whalen, R. Biddle, and P. C. van Oorschot, “The usable security of passwords based on digital objects: From design and analysis to user study,” School of Computer Science, Carleton University, Tech. Rep. TR-10-02, February 2010, https://www.scs.carleton.ca/sites/default/ files/tr/TR-10-02.pdf.

[14] M. Horsch, A. Hulsing, and J. A. Buchmann, “PALPAS — passwordless ¨ password synchronization,” in Proc. ARES 2015. IEEE Computer Society, 2015, pp. 30–39.

[15] M. Horsch, M. Schlipf, J. Braun, and J. A. Buchmann, “Password requirements markup language,” in Proc. ACISP 2016, ser. LNCS, J. K. Liu and R. Steinfeld, Eds., vol. 9722. Springer-Verlag, 2016, pp. 426–439.

[16] J. Kelsey, B. Schneier, C. Hall, and D. Wagner, “Secure applications of low-entropy keys,” in Proc. ISW ’97, ser. LNCS, E. Okamoto, G. I. Davida, and M. Mambo, Eds., vol. 1396. Springer, 1997, pp. 121–134.

[17] ISO/IEC 10118–3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions, 3rd ed., Interna-

tional Organization for Standardization, Geneve, Switzerland, 2004. `

[18] D. Silver, S. Jana, D. Boneh, E. Y. Chen, and C. Jackson, “Password managers: Attacks and defenses,” in Proc. 23rd USENIX Security Symposium, 2014, pp. 449–464.

[19] ISO/IEC 18033–3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers, 2nd ed., International Organization for Standardization, Geneve, Switzerland, 2010. ` [3] Beynon-Davies, P .: ‘Information systems: An introduction to informatics in organizations’ (Palgrave Macmillan, 2002. 2002).