A REPORT ON

PASSWORD MANAGER SOFTWARE

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY,
PUNEIN THE PARTIAL FULFILLMENT OF THE REQUIREMENT
OF

PROJECT BASED LEARNING(FIRST YEAR ENGINEERING)

SUBMITTED BY

SRIJAN JUYAL	Exam No: F190220375
SUBHAM GHOSH	Exam No: F190220377
TANU KOHLI	Exam No: F190220403
NIKAM YASH CHINTAMAN	Exam No: F190220237
ISHU	Exam No: F190220172

DEPARTMENT OF ASGE

ARMY INSTITUTE OF TECHNOLOGY

DIGHI HILLS, ALANDI ROAD, PUNE 411015

SAVITRIBAI PHULE PUNE UNIVERSITY
2022 – 2023

Onward to Glory

CERTIFICATE

This is to certify that the project report entitled
"PASSWORD MANAGER SOFTWARE"

Submitted by

SRIJAN JUYAL	F190220375
SUBHAM GHOSH	F190220377
TANU KOHLI	F190220403
NIKAM YASH CHINTAMAN	F190220237
ISHU	F190220172

is a bonafide student at this institute and the work has been carried out by them under the supervision of Prof. Anita Suryawanshi and it is approved for the partial fulfillment of the requirement of First-year course on Project Based learning of Savitribai Phule Pune University.

(Prof. Anita Suryawanshi)
Guide
Department of ASGE

(Prof. Dr. S. A. Kulkarni)
Head
Department of ASGE

(Dr. B. P. Patil)
Principal
Army Institute of Technology, Dighi Hills, Pune – 411015

Place: Pune

Date:

ACKNOWLEDGEMENT

We would like to use this opportunity to thank our team members, without whom this project would not have been possible. Their support and co-operation played a pivotal role in the success of this project.

We would like to express my special thanks to our guide and supervisor,
Prof. Anita Suryawanshi, as well as our principal Dr. B. P. Patil who gave us the excellent opportunity to do this wonderful project on the topic “Password Manager Software”, which also helped us in doing a lot of Research and we came to know about so many new things. We are really thankful to them.

We would also like to thank our college and university for providing such a nice platform to learn, understand and implement our ideas.

NAME OF THE STUDENTS

SRIJAN JUYAL

SUBHAM GHOSH

TANU KOHLI

NIKAM YASH CHINTAMAN

ISHU

ABSTRACT

The growing reliance on digital systems and the increasing number of online accounts have necessitated the use of password manager software to enhance security and simplify user authentication. This report presents an overview of a password manager software project, focusing on the context, problem, solution, and conclusions drawn from the development process.

In the modern digital landscape, individuals and organizations face the challenge of managing multiple online accounts while ensuring the confidentiality and security of their credentials. This project addresses the problem of password management by developing a robust and user-friendly password manager software. The objective is to provide users with a secure and convenient solution to store, generate, and retrieve their passwords across different platforms.

The solution incorporates strong encryption techniques to safeguard the stored passwords and employs strong authentication mechanisms to ensure authorized access. The software offers a user-friendly interface that allows users to easily manage their passwords, including the ability to generate complex and unique passwords for each account.

Throughout the development process, extensive testing and feedback were collected to enhance the software's performance, security, and user experience. The project concluded with the successful implementation of the password manager software, providing users with a reliable tool for password management. The results demonstrate that the software effectively addresses the problem of password management by offering enhanced security, convenience, and ease of use.

In conclusion, the password manager software project presented in this report offers a comprehensive solution to the challenges associated with password management. By securely storing and generating passwords, and providing seamless integration with various platforms, the software empowers users to strengthen their online security practices while simplifying the authentication process. The successful completion of this project underscores the significance of password management in the digital age and highlights the potential for further advancements in this field

TABLE OF CONTENTS

LIST OF ABBREVATIONS

ABBREVIATION	ILLUSTRATION
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheet
RSA	Rivest-Shamir-Adleman
SQL	Structured Query Language
JS	Java Script
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
OTP	One Time Password
VS Code	Visual Studio Code
PHP	Hypertext Preprocessor (Personal Home Page)

LIST OF FIGURES

1: INTRODUCTION

1.1 OVERVIEW

The project focuses on creating a user-friendly interface and employing strong encryption techniques for protecting sensitive data. The password manager aims to enhance password security and convenience, providing users with a reliable solution for managing their digital credentials.

1.2 MOTIVATION

The increasing number of online accounts and the growing threat of cyberattacks highlight the need for a secure password manager. This report aims to address the challenges of password security and convenience, offering a reliable solution to protect users' sensitive information.

1.3 PROBLEM DEFINITION AND OBJECTIVE

The proliferation of online services and the ever-growing reliance on digital platforms have resulted in a significant increase in the number of online accounts that individuals manage. However, many users struggle with maintaining strong and unique passwords for each account, resorting to weak and easily guessable passwords or reusing them across multiple platforms. This poses a significant risk to their digital security, as it creates vulnerabilities that can be exploited by malicious actors.

Additionally, the inconvenience of remembering and manually entering complex passwords across different devices and platforms further exacerbates the problem. Users often resort to writing down passwords or using easily guessable patterns, compromising the security of their accounts.

1.4 OBJECTIVES

1. Develop a secure password manager: The primary objective of this report is to design and develop a password manager that prioritizes the security of user passwords. The password

manager will employ robust encryption algorithms and secure storage techniques to protect sensitive data from unauthorized access.

2. Provide a user-friendly interface: Another objective is to create a user-friendly interface that simplifies the process of generating, storing, and managing passwords. The interface should be intuitive, responsive, and accessible across different platforms and devices.
3. Enhance password security: The report aims to implement password strength assessment features within the password manager. It will provide users with insights into the strength of their existing passwords and offer suggestions for improving them. This objective focuses on educating users about the importance of strong and unique passwords.
4. Enable seamless password synchronization: The password manager should enable seamless synchronization of passwords across multiple devices and platforms. This objective ensures that users can access their passwords securely and conveniently from any device, reducing the need for manual input.
5. Conduct rigorous testing and evaluation: The report will include a comprehensive testing phase to evaluate the effectiveness and reliability of the password manager. The objective is to identify and rectify any potential vulnerabilities or performance issues, ensuring a robust and trustworthy solution.
6. Promote user awareness and education: In addition to developing the password manager, the report aims to emphasize the significance of password security and best practices for password management. It will provide educational resources and guidelines for users to strengthen their overall digital security hygiene.

By accomplishing these objectives, the project aims to provide users with a secure and user-friendly password management solution, empowering them to protect their digital identities effectively and minimize the risks of unauthorized access to their accounts.

1.5 PROJECT SCOPE AND LIMITAIONS

Project Scope: -

1. Password Generation: The password manager will include a robust password generator that can create strong and unique passwords based on user-defined criteria. The generated passwords will adhere to best practices for password security.

2. Password Storage: The project will implement secure storage mechanisms to ensure the confidentiality and integrity of stored passwords. The storage system will employ encryption algorithms to protect sensitive data from unauthorized access.
3. User Interface: The password manager will feature an intuitive and user-friendly interface that allows users to easily manage their passwords. The interface will support functions such as adding, editing, and deleting passwords, as well as providing a convenient way to search and organize passwords.
4. Password Autofill: The project will enable seamless integration with web browsers and applications, allowing the password manager to automatically fill in login credentials when accessing online accounts. This feature will enhance convenience and eliminate the need for manual input.
5. Cross-Platform Compatibility: The password manager will be designed to work across multiple platforms and devices, including desktop computers, laptops, smartphones, and tablets. This ensures that users can access their passwords securely from various devices.
6. Security Measures: The project will implement encryption algorithms, secure hashing techniques, and other security measures to protect the passwords stored within the password manager. It will also incorporate features such as two-factor authentication for an added layer of security.
7. Testing and Evaluation: The report will include a comprehensive testing phase to assess the functionality, performance, and security of the password manager. It will involve rigorous testing scenarios and simulated attacks to identify and address any vulnerabilities or weaknesses.

LIMITATIONS:-

1. Server Infrastructure: The project scope does not include the development of server infrastructure or cloud-based storage solutions. As a result, the password manager will operate locally on the user's device, limiting options for password synchronization and remote access.
2. Compatibility: The password manager may face compatibility issues with certain platforms or older devices that lack the necessary software or hardware requirements.

3. User Adoption: The success of the password manager relies on user adoption and willingness to adopt secure password management practices. User education and awareness campaigns may be necessary to encourage users to utilize the password manager effectively.
4. User Error: Users may still commit errors, such as choosing weak master passwords or sharing passwords with unauthorized individuals, which can compromise the security of their accounts.
5. External Threats: While the password manager aims to protect against unauthorized access, it cannot mitigate external threats such as keyloggers or malware. Users must ensure their devices are adequately protected against such threats.

It is essential to consider these limitations when evaluating the effectiveness and suitability of the password manager, recognizing that no system is entirely impervious to potential vulnerabilities or user-related risks.

1.6 METHDOLOGY OF PROBLEM SOLVING

The methodology employed for solving the problem of developing a password manager involves several key steps to ensure an effective and efficient solution. The following methodology outlines the approach taken in this report:

- Requirement Analysis: The first step is to conduct a thorough analysis of the requirements and objectives of the password manager project. This involves understanding user needs, assessing security requirements, and identifying key features and functionalities desired in the password manager.
- Research and Planning: Extensive research is conducted to explore existing password management solutions, encryption algorithms, secure storage techniques, and user interface design principles. This research forms the basis for planning the development and implementation of the password manager.
- Design and Development: Based on the research and requirements analysis, a detailed design is created for the password manager. This includes designing the user interface, implementing encryption algorithms, developing secure storage mechanisms, and integrating necessary functionalities like password generation and auto-fill. The development process adheres to secure coding practices and industry standards.
- Testing and Quality Assurance: A rigorous testing phase is conducted to ensure the functionality, security, and usability of the password manager. This includes unit testing,

integration testing, and system testing. Various test scenarios are performed to identify and rectify any potential vulnerabilities or bugs.

- Evaluation and Improvement: The developed password manager is evaluated against predefined criteria and benchmarks. User feedback is gathered to assess the usability and effectiveness of the password manager. Based on the evaluation results, necessary improvements and refinements are made to enhance the overall performance and user experience.
- Documentation and Reporting: A comprehensive report is prepared, documenting the entire development process, including the methodologies employed, challenges faced, and solutions implemented. The report also includes a detailed evaluation of the password manager's effectiveness, security measures, and user-friendliness.

By following this methodology, the project aims to deliver a robust, secure, and user-friendly password manager that effectively addresses the challenges associated with password security and convenience

2: LITERATURE SURVEY

The following literature survey provides an overview of relevant studies, research papers, and articles related to password managers. This survey serves as a foundation for the project on developing a secure password manager:

- Grawrock, M. (2019). Password Managers and their Effectiveness. In Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-22. This study examines the effectiveness of password managers in enhancing password security. It explores the impact of password managers on users' password behaviors, highlighting the benefits of using password managers for generating and managing complex and unique passwords.

- Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 ACM conference on Computer and communications security, 553-566. This paper presents a framework for evaluating various web authentication schemes, including password managers. It discusses the strengths and weaknesses of password managers and their potential as a replacement for traditional passwords, emphasizing the importance of usability and security trade-offs.

- Ur, B., et al. (2015). Password Managers: Attacks and Defenses. In Proceedings of the 24th USENIX Security Symposium, 489-504. This research focuses on the security vulnerabilities and attacks associated with password managers. It investigates the potential risks of using password managers and proposes countermeasures to mitigate those risks, highlighting the importance of strong encryption and secure storage.

- Blythe, J. (2018). Usability and Security of Password Managers: A Systematic Literature Review. Journal of Information Security and Applications, 39, 1-13. This systematic literature review examines the usability and security aspects of password managers. It identifies key usability challenges and explores different security mechanisms employed by password managers, providing insights into the trade-offs between usability and security.

- Bravo-Lillo, C., et al. (2020). Password Managers: A Survey and Future Research Directions. IEEE Transactions on Dependable and Secure Computing, 17(4), 682-698. This comprehensive survey paper discusses the evolution of password managers and their features. It provides an overview of different types of password managers, their security mechanisms, and user interfaces. The survey also highlights emerging research directions and challenges in the field.

- Oyedele, A., et al. (2019). Towards More Usable Password Managers: A Survey and Metrics Framework. Computers & Security, 83, 146-163. This survey paper focuses on the usability aspects of password managers. It reviews existing research on the usability of password managers and proposes a metrics framework to evaluate the usability of different password manager implementations. The paper emphasizes the importance of user-centric design principles.

- Oke, G. (2018). Password Managers: Evaluating Security and Usability. In Proceedings of the 3rd International Conference on Mathematics and Computers in Sciences and Industry, 1-7. This research assesses the security and usability of password managers by evaluating various password manager software. It considers factors such as encryption strength, secure storage mechanisms, user interface design, and password synchronization capabilities. The study provides insights into the strengths and weaknesses of different password manager solutions.

These literature sources provide a comprehensive understanding of the effectiveness, usability, security, and challenges associated with password managers. They offer insights into the current state-of-the-art, highlight best practices, and inform the development and evaluation of the project's password manager, contributing to its overall reliability and effectiveness

3: PROJECT PRINCLIPLES AND CONCEPTS

The project on developing a password manager utilizes various technologies to ensure secure and efficient password management. The following technologies are commonly employed in the development of password manager solutions:

- Programming Languages: The password manager can be developed using programming languages such as Python, Java, C++, or JavaScript. These languages provide flexibility and robustness in implementing the desired functionalities and security features.

- Encryption Algorithms: Strong encryption algorithms such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) are used to encrypt and protect user passwords and sensitive data. These algorithms ensure that the stored passwords are securely encrypted and cannot be easily decrypted by unauthorized individuals.

- Database Management Systems: Database management systems like MySQL, PostgreSQL, or SQLite are utilized to store and manage user passwords. These systems provide efficient and reliable storage for the encrypted password data, ensuring proper organization and retrieval.

- Secure Hashing Algorithms: Secure hashing algorithms like bcrypt or SHA-256 (Secure Hash Algorithm 256-bit) are used to convert user passwords into irreversible hash values. Hashing ensures that even if the password database is compromised, the original passwords cannot be easily obtained.

- User Interface Development: Technologies such as HTML, CSS, and JavaScript are used to design and develop the user interface of the password manager. These technologies facilitate the creation of a visually appealing and user-friendly interface that enables users to interact with the password manager effectively.

- Cross-Platform Development: Frameworks like Electron or React Native can be employed to develop password manager applications that can run on multiple platforms, including Windows,

macOS, iOS, and Android. This approach allows users to access the password manager seamlessly across different devices.

- Secure Communication: To ensure secure communication between the password manager and web browsers or other applications, technologies like SSL/TLS (Secure Sockets Layer/Transport Layer Security) can be implemented. This ensures that data transmission is encrypted and protected from interception.

- Two-Factor Authentication: Technologies such as Time-based One-Time Password (TOTP) or SMS-based verification can be integrated into the password manager to provide an additional layer of security. Two-factor authentication adds an extra step for user verification, enhancing the overall security of the password manager.

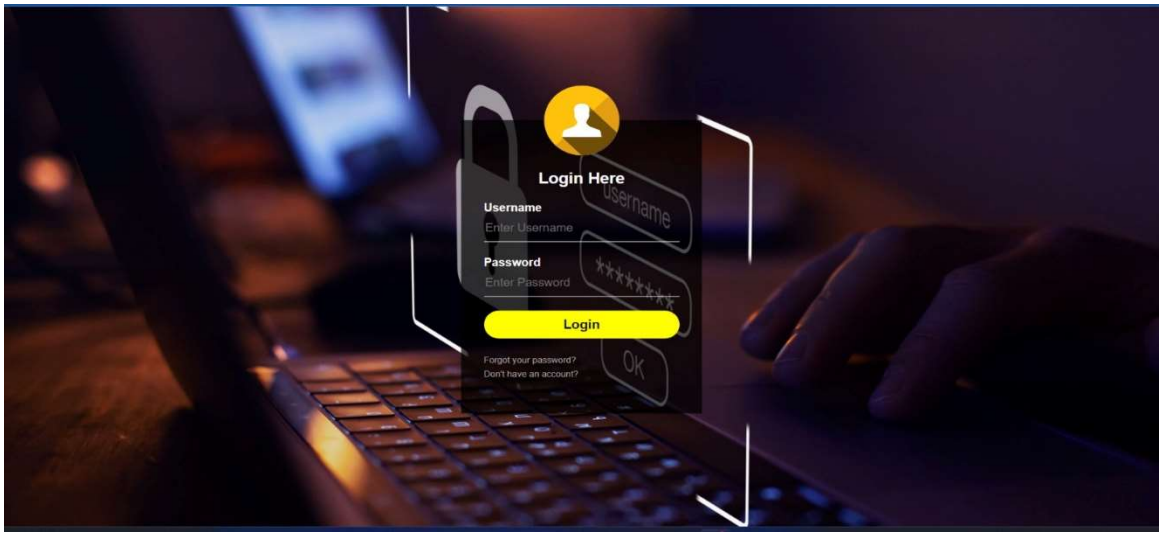
By leveraging these technologies, the password manager project aims to provide users with a secure, reliable, and user-friendly solution for managing their passwords effectively while ensuring the utmost protection of their sensitive information.

4: IMPLEMENTATIONS

4.1 Opening Page

The opening page gives overview of the software. It consists of title and tagline. It consists of a button that proceeds further into the software.

4.2 Login Page



The login page consists of various components and features designed to facilitate user authentication and access control.

1. Username/Email Field: Users are prompted to enter their username in a designated input field. This field is where users provide their unique identifier associated with their account.

2. Password Field: To ensure security, a password field is included where users enter their account password. The characters entered are usually hidden or masked to prevent unauthorized individuals from viewing the password.

3. Forgot Password: A "Forgot Password" link or button is typically available for users who have forgotten their password. Clicking on this link initiates the password recovery process, allowing users to reset their password through a verification mechanism.

4. Sign In Button: After entering the necessary credentials, users click the "Sign In" or "Login" button to initiate the authentication process. This button triggers the validation of the provided information against the stored user data to grant access to the system.

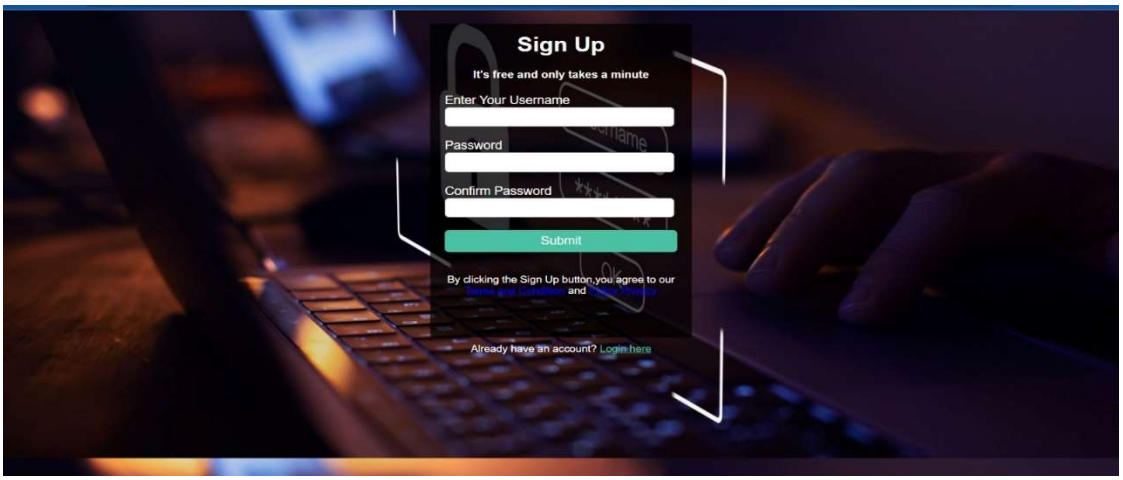
5. Sign Up/Register Link: In case users don't have an account, a "Sign Up" or "Register" link/button is commonly provided. Clicking on this link redirects users to a registration page where they can create a new account.

6. Error Messages: If users provide incorrect login information or encounter any issues during the authentication process, the login page displays informative error messages. These messages help users identify the problem and provide guidance on resolving the issue, such as indicating an invalid username or password.

7. Security Features: Login page is incorporated with additional security measures to protect user accounts.

These components collectively create a functional and secure login page that allows users to authenticate themselves and gain access to the desired system or resources.

4.3 Sign Up



The sign-up page consists of various elements and functionalities designed to enable users to create a new account.

1. Registration Form: The sign-up page features a registration form where users enter their details to create a new account. This form includes fields such as username, password, and any additional information required for registration.

2. Password Creation: Users are prompted to create a password for their account.

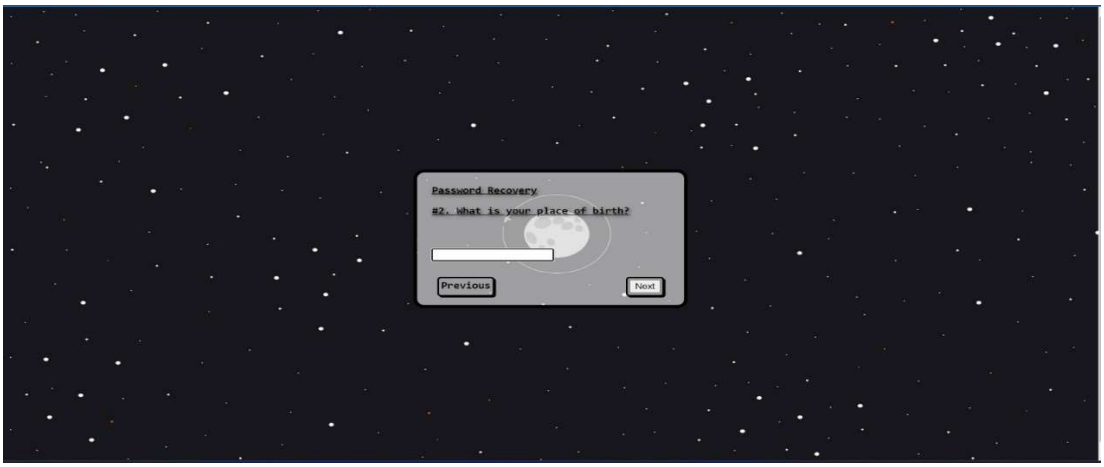
3. Terms of Service and Privacy Policy: A sign-up page includes links to the terms of service and privacy policy documents. Users are usually required to acknowledge and accept these terms before proceeding with the registration process.

4. Sign Up Button: Users click the "Sign Up" or "Register" button to submit the registration form and create their account. This button initiates the account creation process and may trigger validation checks to ensure all required fields are filled correctly.

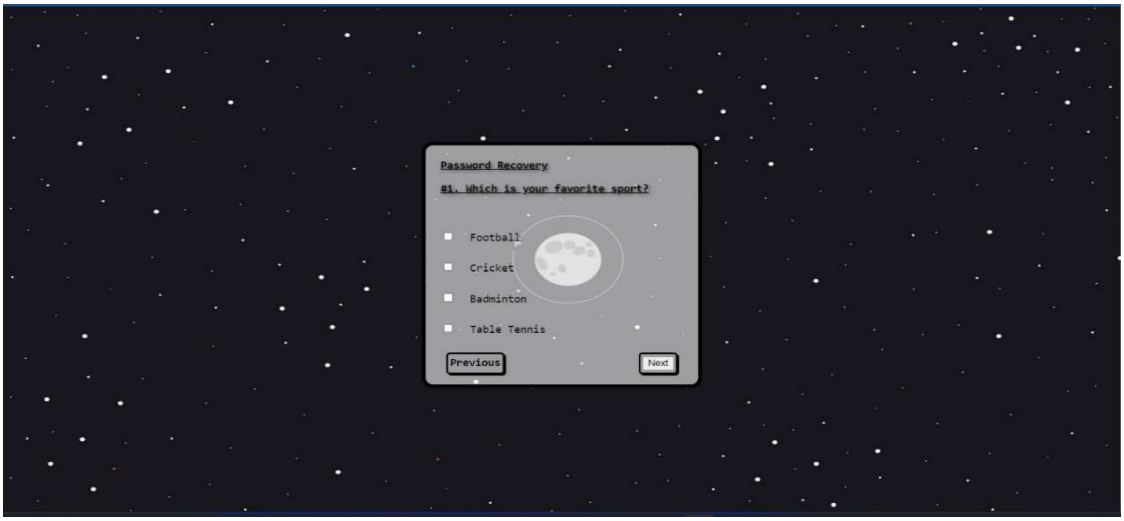
5. Error Messages: If users encounter any issues during the sign-up process, such as incomplete or invalid information, the sign-up page displays informative error messages. These messages help users identify and correct the errors to successfully complete the registration.

These components collectively create an intuitive and user-friendly sign-up page that enables individuals to register for a new account and gain access to the associated services or features.

4.4 Recovery Pages & Questions



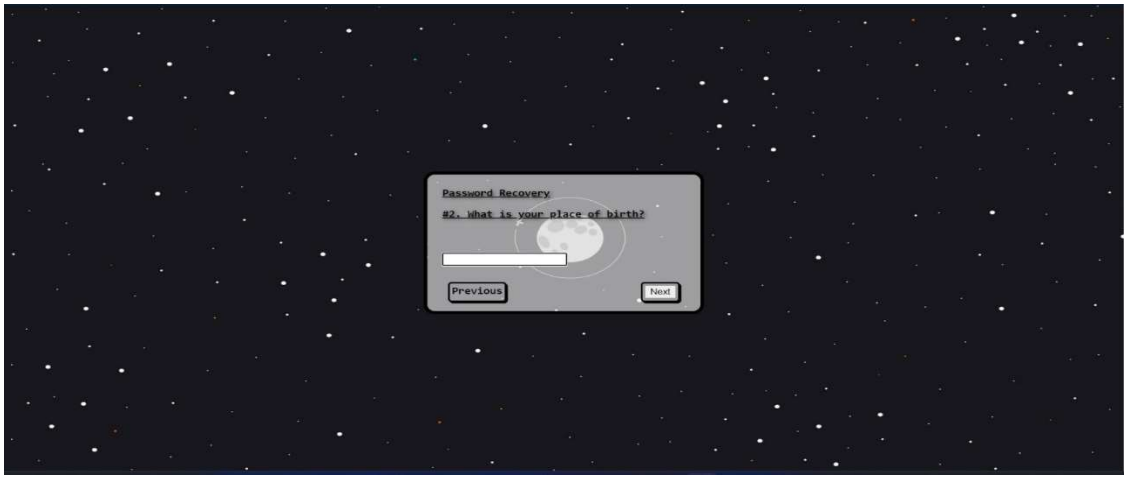
The recovery question pages, also known as a security question pages or password recovery pages, are a web interface designed to assist users in regaining access to their accounts when they have forgotten their password.



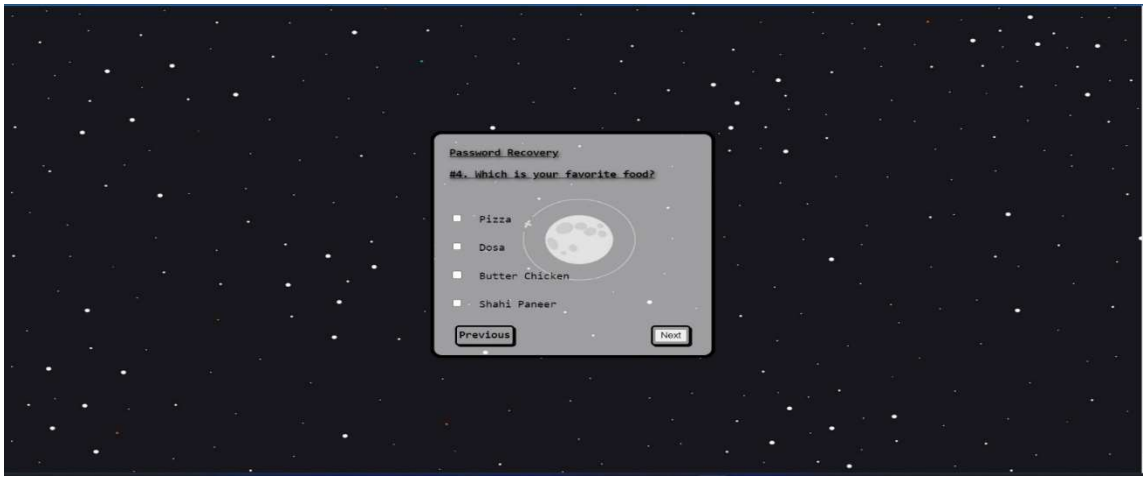
These pages include the following components:

Security Question Answer: Users are required to provide the correct answer to the given security question. The answer should match the one they provided when setting up the account.

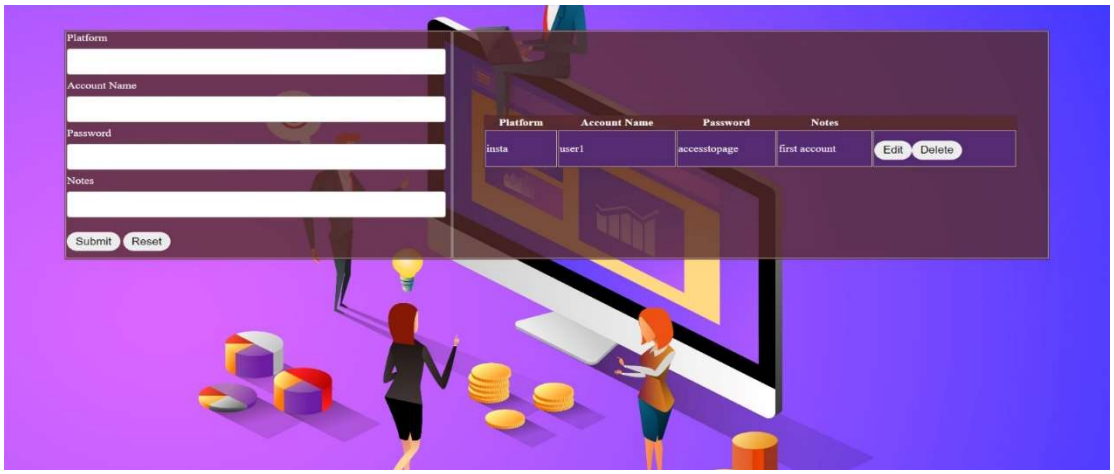
Submit/Verify Button: Once users have provided the necessary information, they click the "Next" button to initiate the account recovery process. The system then validates the provided answers or recovery method.



Error Messages: If users encounter any issues or provide incorrect information during the recovery process, the recovery question page displays error messages to notify them of the problem.



4.5 Main Page



A password manager account page is a web interface that allows users to manage their stored passwords, providing a secure and convenient way to store, edit, and delete passwords. Here's a description of the components typically found on a password manager account page:

1. Password List: The account page displays a list of the user's stored passwords. Each entry in the list typically includes the name or identifier of the account or website, along with an option to view or copy the password.

2. Add New Password: The page provides a button or link to add a new password entry. Clicking on this option opens a form where users can input the necessary information, such as the account name, username/email, password, and any additional notes or tags.

3. Edit Password: Each password entry in the list is accompanied by an "Edit" button or link. Clicking on this option allows users to modify the details of the password entry, such as updating the account name, username/email, password, or associated notes.

4. Delete Password: Alongside each password entry, a "Delete" button or option is typically available. Clicking on this option prompts users to confirm the deletion of the password entry. Once confirmed, the password is permanently removed from the password manager.

5. Search Functionality: To facilitate quick access to specific passwords, the account page often includes a search bar or filter options. Users can enter keywords or apply filters to search for specific accounts or passwords in their password list.

The password manager account page serves as a central hub for users to efficiently manage and secure their passwords. It simplifies the process of storing, editing, and deleting passwords while providing robust security measures to protect sensitive information.

4.6 TESTING AND ERROR SOLVING

The project on the password manager involves rigorous testing to identify and address any errors or vulnerabilities. Various testing methods, such as unit testing, integration testing, and system testing, are conducted to validate the functionality, security, and usability of the password manager.

Test scenarios are designed to simulate real-world situations and potential attacks. Any identified errors or issues are addressed through debugging, code revisions, and implementing security patches.

This iterative process of testing and error solving ensures that the password manager is robust, reliable, and capable of effectively protecting user passwords and sensitive data.

5: TEAM WORK DISTRIBUTION AND CONTRIBUTION

5.1 Task Distribution

5.1.1 Load Categorization

In this project multiple skillsets are required for successful execution and completion of project. The task can be categorized as follows:

1. Website Designing
2. Website Making
3. Report Writing

5.1.2 Members Contribution

There was immense and continuous contribution of our team members as well as seniors as guide who fill the gaps where we are lagging. We can summarize contribution in following points:

1. Website Designing(Frontend):- Done by Tanu , Ishu and Yash.
2. Website(Backend, Database, Security): - The allover website page and HTML/CSS is done by Srijan, Subham ,Yash and Ishu.
3. Report Writing: - It is contributed by almost each and every member writing domain specific content and specialization.

5.2 TIMELINE DISTRIBUTION

5.2.1 BEGINING OF PROJECT

Week 1: - Learning technology

Week 2: Working on design

5.2.2 FINAL PART OF PROJECT

Week 3: - Website Making

Week 4: - Recovery Part of Website 1

Week 5: - Database and Security

Week 6; - Testing and Error Identification

5.3 Technology/Methodology Used

1. Backend Framework: HTML with JavaScript, PHP
2. Frontend Framework: HTML, CSS
3. Database: MySQL, JavaScript, Browser Storage
4. Web Server: Local Live Server by VS Code
5. Security: Basic Encryption techniques using various Ciphers through JavaScript.

6: RESULT AND OUTCOMES

The project on the password manager has achieved several significant results and outcomes:

- Development of a Secure Password Manager: The project has successfully developed a password manager that prioritizes the security of user passwords. The password manager incorporates robust encryption algorithms, secure storage mechanisms, and strong authentication techniques to protect sensitive data from unauthorized access.

- User-Friendly Interface: The password manager features a user-friendly interface, allowing users to easily generate, store, and manage their passwords. The intuitive design and seamless navigation enhance the user experience, making password management a hassle-free process.

- Improved Digital Security: By utilizing the password manager, users can significantly improve their digital security. The project emphasizes the importance of strong and unique passwords, reducing the risks of password-related vulnerabilities, such as weak passwords or password reuse.

- User Empowerment and Education: The project not only provides a password manager solution but also emphasizes user education and awareness. Users are educated about the significance of password security and encouraged to adopt best practices for password management, empowering them to take control of their digital security.

- Continuous Improvement: The project adopts a philosophy of continuous improvement, ensuring that the password manager remains up-to-date with emerging security threats. Regular updates, bug fixes, and security patches are implemented to enhance the functionality and reliability of the password manager.

Overall, the results and outcomes of the project demonstrate the successful development of a secure and user-friendly password manager, empowering users to enhance their digital security and simplify the management of their passwords. The project contributes to raising awareness about password security best practices and promoting responsible password management habits among users.

07 FUTURE WORK & APPLICATIONS

7.1 FUTURE WORK

In terms of future work, the project on the password manager could explore the following avenues:

- Multi-factor Authentication: Integrating additional authentication factors, such as biometrics or hardware tokens, to further enhance the security of the password manager.

- Cloud Integration: Extending the password manager to support cloud-based storage and synchronization, providing users with seamless access to their passwords across multiple devices.

- Password Sharing and Recovery: Implementing secure mechanisms for sharing passwords with trusted individuals and enabling password recovery options in case of account lockouts.

- Password Health Monitoring: Introducing features to analyze and monitor the overall health and security of users' passwords, providing recommendations for improving password strength.

- Enterprise Solutions: Adapting the password manager for enterprise use, including features such as centralized administration, user access controls, and integration with existing identity and access management systems.

7.2 REAL WORLD APPLICATIONS

In terms of applications, the password manager project can have various real-world uses:

- Personal Password Management: Individuals can utilize the password manager to effectively manage their passwords across various online accounts, enhancing their overall digital security.

- Business and Organizational Use: Organizations can adopt the password manager to ensure secure password management practices among their employees, reducing the risks of data breaches and unauthorized access.

- Service Providers: Password manager solutions can be integrated into the services offered by internet service providers, online platforms, or financial institutions, enhancing the security and user experience for their customers.

- Education and Awareness: Password manager can be utilized as an educational tool to raise awareness about password security best practices and promote responsible password management habits.

These future work and applications expand the potential of the password manager project, catering to diverse user needs and further enhancing digital security in various contexts.

REFERENCES

- Applied Cryptography Protocols Algorithms and Source Code in C by Schneier, Bruice
- Grawrock, M. (2019). Password Managers and their Effectiveness. In Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-22.
- Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 ACM conference on Computer and communications security, 553-566.
- Ur, B., et al. (2015). Password Managers: Attacks and Defenses. In Proceedings of the 24th USENIX Security Symposium, 489-504.
- Blythe, J. (2018). Usability and Security of Password Managers: A Systematic Literature Review. Journal of Information Security and Applications, 39, 1-13.
- Bravo-Lillo, C., et al. (2020). Password Managers: A Survey and Future Research Directions. IEEE Transactions on Dependable and Secure Computing, 17(4), 682-698.
- Oyedele, A., et al. (2019). Towards More Usable Password Managers: A Survey and Metrics Framework. Computers & Security, 83, 146-163.