International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 11 | November - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Password and Notes Manager in Java

Aanchal
Student
Computer Science and Engineering
Chandigarh University , Mohali
India

Er.Ritu
Assistant Professor
Computer Science and Engineering
Chandigarh University , Mohali
India

Himanshu Chauhan
Student
Computer Science and Engineering
Chandigarh University , Mohali
India

Saakar Munjial
Student
Computer Science and Engineering
Chandigarh University , Mohali
India

Aryan Kaushal
Student
Computer Science and Engineering
Chandigarh University , Mohali
India

Shivani Pradhan
Student
Computer Science and Engineering
Chandigarh University , Mohali
India

ABSTRACT
These days many web accounts for email, banking, blogging, online shopping, creating new accounts etc. have a problem when it comes to selecting passwords for all these different accounts. Since each of these accounts requires a single password, if the hacker manages to obtain one of the passwords, he/she will easily access the other's user account including all details. However, when user use various passwords for different systems, they may select weak or passwords which they can remember easily. It raises the operational and user support cost related to password resets.
So, to overcome with this issue we are working to develop a secure password manager that can store multiple user accounts and passwords. The password manager provides excellent usability and user-friendliness for users and protect data to ensure optimum security for the user.
It's an intuitive, straightforward GUI-based program. Its numerous features improve the user experience. Passwords for several apps can be kept in this program. Information such as the application or website, name, login, password, and email address are needed to keep the passwords secure.

Keywords
Password Manager, Optimum, GUI

1,INTRODUCTION
Passwords are an essential component for providing security. When it comes to protecting practically all data including networks, servers, databases etc. passwords serve as a first line of protection. Password manager gives the ability to save, generate, and enter strong one-of-a-kind passwords. User don't have to worry about forgetting or misplacing their passwords because password managers keep track for them.
Using a password and notes manager is essential because:
1.It has an intuitive user interface that makes it simple for users to comprehend and utilize in an efficient manner.
2. It improves security by shielding from unwanted access
3. By creating a strong password automatically and doing away with the necessity for human password formation, it saves time.
The Java password and note manager tackles a pertinent modern problem—that is, the growing significance of data security and privacy. The firm is continuously at danger of data breaches and illegal access to sensitive information as a result of the increasing cyber risks that come with technological advancements. This concept aligns with current concerns about cybersecurity threats, data privacy, remote work, and digital cooperation.
In its most basic form, a password manager is a program that stores a user's login credentials, such as their username and password, to lessen the cognitive strain of having to remember numerous different login credentials. This collection of passwords is called a password vault. Ideally, the vault should be kept encrypted, and the master password—a password selected by the user—should provide the encryption key. If desired, the password vault can be stored online, enabling synchronization across many devices. In addition to storing user-selected passwords, the majority of password managers available today also let users create new passwords.
In this project app is created in which there is a login page, if a user is new then he/she first of all registered herself/himself. After getting registered he/she able to login with that page and then a page open where he/she can store his/her passwords along with the websites name also if he/she wants to add or delete or want to update can update with the given options on the page below.

2.Related Work
The field of study on password managers is closely related to practical cryptography and penetration testing, much of our work draws on academic papers about the security of more widely used password managers, as well as penetration testing reports from security auditing teams. Will continue to refer to. However, we will also include references to specific papers that demonstrate proof of concept or make other improvements to the field. Crafted by Halderman et al. from 2005 incorporated the execution and evidence of idea of a secret key supervisor in an internet browser; their work remembered an illustration of an execution for Firefox.
Happening to the pattern of safety examination, Li, He, Tune, and Akhawe furnish us with data on notable secret key chiefs like LastPass and RoboForm. Exceptional commitments to the auto-fill highlight in generally utilized secret key administrators like LastPass and KeePass,as well as those coordinated into internet browsers like Google Chrome and Safari, have been made by Silver, Jana, Chen, Boneh, and Jackson They found serious defects in the auto-fill usefulness, including infusions, secret key sync takes advantage of, and iFrame clear assaults.

Their endeavors would essentially affect the strategies that auto-fill carries out. To show a portion of the hidden issues that appear to be making secret key chiefs developing progressively essential, the endeavors of Gaw and Felten would uphold review measurable examination held in Princeton College. Felten and Gaw found that people much of the time involved similar passwords for lesser-significant
sites and conjecture that this pattern will increment as additional individuals go online. Accounts develop. Members were found to be uninformed to the risks this pattern stances to security. Furthermore, they found that there was an absence of energy for utilizing secret key managers. Zhao, Yue, and Sun's work inspected the developing pattern of distributed computing and dissected the weaknesses of RoboForm and LastPass. They had the option to distinguish dangers like certifications being put away in plaintext on cloud servers and gave counsel to both item creators on the most proficient method to more readily get their information and items.
Gasti and Rasmussen are referenced to wrap up the pertinent work; among their commitments is a trailblazer in the examination of secret phrase director data set formats.as the title of the paper suggests: "On the Security of Secret word Manager “Table Design What Rasmussen and Gasti found was that despite the fact that few secret word chiefs vary from one another, they basically utilized similar data set structure. Additionally, they found numerous shortcomings in each secret phrase supervisor they investigated.

3.Literature Survey

A Java-based password and note management project's background investigation comprises a detailed analysis of the market environment, accounting for prior research, technological advancements, and user needs. Below is a summary of the background research for this kind of project:

Security Environment: It's critical to comprehend how cybersecurity threats and password-related vulnerabilities have evolved over time.
Examine the most recent hashing techniques, access control plans, and encryption algorithms to guarantee robust data security.

Password manager trends
Looking at well-known note-taking and password apps on various platforms will make it easier for you to identify common features, security best practices, and usability standards in current solutions. Examining user feedback will assist you in identifying the benefits and drawbacks of the available solutions.

3.1 Timeline

Bruce Schneier's Password Safe, which was made available as a free download on September 5, 1997, was the first password manager program created with the intention of safely storing passwords.
2010: Java's Introduction to Security
It is acknowledged that Java has strong security features, which provide the foundation for developing secure applications.
2012: Password managers began to appear
Password managers become more and more popular as cybersecurity awareness grows, highlighting the importance of safe data storage.
2015: A Boom in Security Research
To improve overall security, a great deal of research is done on hashing algorithms, access control, and encryption algorithms in password management systems.
2016: Development of Java UI
As Java's graphical user interface (GUI) capabilities grow, more user-friendly and intuitive password and note manager interfaces are produced.
2018: Put Usability First
The focus of research is shifting to Java-based password and note managers in an effort to strike a balance between security and usability, with a particular emphasis on how important user experience is.
2020: Two-Factor Verification
Enhancing the security of password and note manager access becomes a primary focus with the implementation of multi-factor authentication.
Cloud-Based Solutions in 2023
Cloud-based password managers are becoming more and more popular, and Java is essential to enabling safe data synchronization between devices.

3.2 Proposed Solutions

Key features, design considerations, and security measures are typically included in the proposed solution for a Java-based password and note manager project. This is a summary of a previous project solution that was suggested:
Key attributes:
o Secure Data Storage: To guarantee the safe storage of notes and passwords, use strong encryption algorithms.
o User Authentication: For improved user verification, include multi-factor authentication (MFA) and consider incorporating biometric technologies.
o Intuitive GUI: Utilize Java's GUI features to create a graphical user interface that is easy to use and intuitive for users to interact with.
o Cross-Platform Compatibility: Take advantage of Java's platform independence to make sure the application runs without a hitch on various operating systems.
o Cloud Integration: Offer cloud storage with robust encryption for both in-transit and at-rest data.

3.3 Review Summary

The proposed Java-based password and note manager project provides a feature-rich, end-to-end solution with an emphasis on enhancing security and user experience. The use of encryption techniques ensures secure data storage, and the implementation of multi-factor authentication (MFA) significantly increases total security. Through the use of Java's platform neutrality, users can easily access content on multiple platforms and operating systems. The flexibility of cloud integration for data synchronization and storage, along with the addition of a password generator and note management, increase the application's adaptability.
The initiative is not without potential challenges, though. Strong security measures like MFA might make it difficult for users to accept them at first, especially if they value convenience. The dependence on external cloud services raises concerns about data privacy and the long-term viability of the service. Graphical user interface design decisions are arbitrary, so user feedback is necessary to make them better all the time. Furthermore, adding note-taking features and other features could make things more complicated and deviate from the simplicity that many users desire in password managers.
Notwithstanding these obstacles, the project is regarded as having been highly successful in addressing the primary issues with note and password management. The project is positioned as a comprehensive solution due to its features, security measures, and user-focused design. It is recommended that security and user convenience be balanced, that external dependencies be carefully managed, and that it be continuously improved based on user feedback. All things considered, the project appears to have potential in offering a secure, uncomplicated, and adaptable way to manage private notes and passwords.

4.Methodology

In this project, system stores the passwords along with the websites name so that user can easily access the harder passwords. The storing of passwords and notes is backend in java in which user can delete, update, save and passwords and in the front end Html and css is used in which user first registered and then login with his/her username and passwords.

4.1 Design Selection

An important part of developing a Java-based password and note management system is choosing the appropriate design. The architecture, data storage, user interface, and security are just a few of the elements that are included in the design. An outline of the design selection procedure is provided below:

1. Architecture Selection: Client-Server or Local Application: Choose if the application will be a local application, storing data on the user's device, or a client-server model, storing data on remote servers. This decision may affect accessibility and security.

2. Database Design: Relational or NoSQL: Select whether to store user data in a relational database (such as MySQL or PostgreSQL) or a NoSQL database (such as MongoDB). The choice should take the project's performance requirements and scalability into account.

3. Security Measures: ▧ Encryption: To safeguard user data, use end-to-end encryption.

▪ Access Control: Establish access control methods to stop unwanted access to confidential data.

▪ Secure Password Storage: Use a secure technique, like salting or hashing, to store user passwords.

Select the authentication technique you want to use, such as multi-factor, biometric, or password-based.

4. User Interface Design: ▪ Responsive Design: Make sure the interface is accessible and responsive on various screens and devices.

▪ Intuitive Navigation: Create a user interface that is easy to use and has features and menus that are arranged logically.

▪ Customization: Take into account letting users alter the application's design and structure.

4.2 Design Constraints

A Java-based password and note management project's design is a complex process that calls for careful consideration of a number of design constraints. These limitations are crucial in determining the architecture, functionality, and general user experience of the project. The main design limitations that are essential to the effective development and implementation of this kind of project are outlined below.

1. Constraint on Data Privacy and Compliance:

Design Restraint: In order to protect user data and uphold moral and legal principles, the project must closely conform to data privacy laws and industry-specific compliance standards.

Explanation: Any application that handles sensitive user data, like passwords and private notes, must consider data privacy and compliance.

o The project must abide by all applicable data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and other local, national, and industry-specific requirements.

o Design limitations concerning compliance and data privacy include:

▪ Secure Data Encryption: Robust encryption algorithms must be used to store and transport user data, including passwords and notes, in a secure manner.

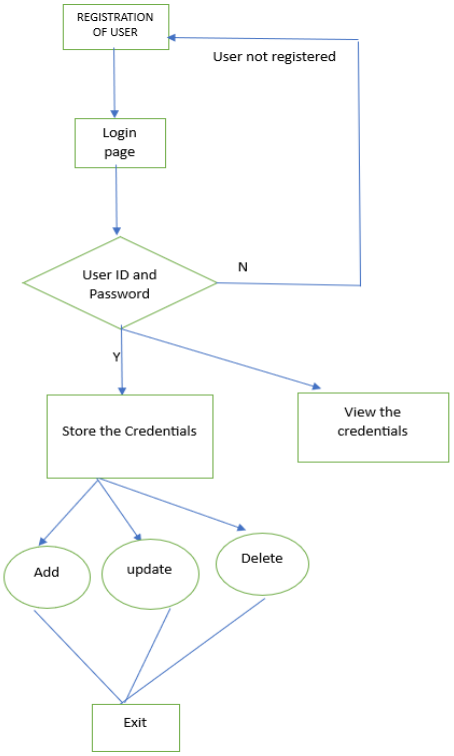
▪ Consent and Transparency: Users must be made aware of the procedures used for data collection, processing, and storage. Additionally, their express consent must be sought before handling any personal information.

▪ Data Retention and Deletion: In accordance with legal requirements, the project must establish data retention guidelines and provide users the option to remove their data.

▪ Audit Trails: For compliance and auditing purposes, keep track of data access and modifications.

▪ Notification of Data Breaches: The project must follow legal procedures for informing authorities and impacted users in the event of a data breach.

4.3Design Flow



Implementation steps:

1.Registration

- To store passwords, user need to registered first if he/she is not registered.
- B**y** adding their email id, creating a password user can registered.

2.Login

- After registration user can login with their user id and password.
- If the password and user id is correct then it will get login into main menu

3.Save Information

- User can save their passwords along with thw websites as much as they want.
- User can update, Add and delete data also whenever they want by login with their registered user id and passwords.

4.Exit

5.Conclusion

These days, password managers are the most underappreciated software. Though they are more important than ever, people do not realize how much they need them. The number of hacking attempts is increasing daily and will continue to rise in the future if nothing is done. Businesses are making every effort to safeguard their servers against these intrusions, but users remain susceptible when they use easy-to-crack passwords. A large number of recent hacking attempts have come from user-generated content. The only way to help these users remember

complex passwords is to use password managers. We want to raise awareness of this crucial software and make the code available as open-source so that personal security continues to advance just a little bit in the future.

6.Refrences

1. https://copyassignment.com/password-and-notes-manager-in-java/
2. https://www.w3counter.com/globalstats.php
3. https://www.tutorialspoint.com/html5/html5_indexeddb.htm
4. https://www.html5rocks.com/en/tutorials/file/filesystem/
5. http://canadiancloudbackup.com/safe-safe-aes-256-encryption-data/
6. **Churi, Prathamesh P.; Ghate, Vaishali; Ghag, Kranti -- [IEEE 2015 International Conference on Science and Technology (TICST)**
7. **Pathum Thani, Thailand “”Jumbling- Salting: An Improvised Approach for Password Encryption [17] Password Manager - Automatic Password Change Using Headless Browsers : A Survey**
8. https://www.kashipara.com/project/idea/java/notes-and-password-management_4016.html
9. https://www.scribd.com/document/632048365/Passwords-and-notes-manager-in-android-application

10.https://www.crio.do/projects/java-android-notes-password-manager/