**Password Management System**

**Akansha Gupta, Vaishali Jeenwal, Akshitha Kamshetty**

**Information Systems, Northeastern University**

**{Gupta.akan, jeenwal.v, kamshetty.a}@northeastern.edu**

**Abstract:**

Managing passwords in the digital world is a big concern. That's why we created a strong Password Management System (PMS). We explored and built this system using JavaFX for a user-friendly look and File I/O to keep passwords safe with encryption. Our main goal is to handle passwords securely. PMS has useful features like easily changing passwords, copying and pasting them, and making strong random passwords. This project makes using passwords safer and more comfortable.

Our report covers a lot of things. We start by looking at the problem closely and checking similar work that has been done. We explain how the system is designed, including pictures of how it looks and diagrams that show how it works. We also talk about how we actually built the system. We used JavaFX to make it nice to use, and we added encryption to keep passwords really safe. We even made it generate, edit, and copy passwords.

We tested the system and found that it works well, which we can prove with a study we did with some people. Their feedback helped us make the system even better. We also talk about what our project means in a bigger sense, looking at how it affects how easy passwords are to use and how safe they are.

Finally, we talk about what could come next. We have ideas for making the system even better and more useful. Our project is a mix of different skills, combining what we know about computers and software to make a solution that keeps people's digital information safe and easy to manage.

**Keywords:** Password Management System, JavaFX, File I/O, Encryption, User Interface, Security, Generator

**Problem Description:**

Authentication is the process of providing proof that a user is actually who they say they are. Authentication systems are based on the use of a physical token (something you have), a physical characteristic (something you are), or secret knowledge (something you know) that can uniquely distinguish a user. The most common type of authentication in use today is a password, which is based on something that is only known by the user and thus prevents imposters from impersonating the user.

Yet, despite their widespread use, passwords provide a weak degree of protection and undermine the system

Schneier (2004) says that “systems are only as secure as the weakest password”.

The weakness of passwords centers on human memory. Human beings can memorize only seven (plus or minus two) “chunks” of information. As more items are added to memory, the number of items that are forgotten increases

Remembering passwords is tough because they need to be strong to keep bad guys out. But strong passwords can be hard to remember. People have lots of accounts and each one needs a password. Research shows that most people have many passwords. Some even have more than a dozen! This makes it really hard to remember all of them.

To make things easier, some people take shortcuts. They might use simple passwords like "12345" or use the same password for different accounts. This isn't safe, though, because if one password is guessed, the others are at risk too.

People even write down their passwords, which is risky. The problem gets worse when rules force us to change passwords often. This means we have to remember new passwords all the time. All these challenges can lead to weak passwords or using the same one everywhere.

Research shows that as people get more online accounts, they just reuse passwords instead of making new ones. So, even though online accounts increase, unique passwords don't.

In the end, the problem is that most people don't try to remember complicated passwords. They'll pick easy ones or write them down, which makes it easier for hackers. This is why passwords can be a big security problem.

(Based on Schneier's quote: "The problem is that the average user can’t and won’t even try to remember complex enough passwords to prevent dictionary attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they’ll choose a lousy one. If you force them to choose a good one, they’ll write it on a Post-it and change it back to the password they changed from last month. And they’ll choose the same password for multiple applications" - 2004)

In response to the multifaceted challenge of password management, we have developed the Password Management System (PMS) project. Our primary goal is to provide a robust and user-friendly solution that addresses the shortcomings of traditional password practices. The PMS is designed to streamline the process of managing passwords, offering a secure and organized approach. Imagine having a dedicated vault for all your passwords, accessible through a single master password. The PMS employs advanced technology to ensure both ease of use and enhanced security. We have created an intuitive interface that simplifies interactions with the system, akin to a user-friendly computer program. Additionally, we have integrated encryption mechanisms that fortify password protection, guarding against unauthorized access. Beyond technology, our project extends to a comprehensive study to gather user feedback and insights, allowing us to continually refine and optimize the system.

In essence, the Password Management System aims to empower users by alleviating the challenges associated with password management. It provides a reliable and efficient means to generate, store, and retrieve passwords securely, reducing the risk of breaches and unauthorized access. By offering a convenient and safeguarded solution, our project seeks to enhance the overall online experience, ensuring that users can navigate the digital landscape with confidence and peace of mind.

**Analysis:**

In this section, we present a summary and analysis of the existing previous works, and findings, that are relevant to our password management application. This analysis helps us understand the context and significance of our project and identify potential areas for improvement.

The provided references discuss various aspects of password management systems, their effectiveness, privacy preservation, and user reactions. "**Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers**" by Quentin Stafford-Fraser explores the use of semantic annotations to enhance password managers' effectiveness. Nooruldeen Qader focuses on privacy preservation and personalized password management against untrusted browser origins.

In "**A Study for an Ideal Password Management System**" by Shivam K. Shinde and Mohit V. Deshpande, the authors delve into the design and features of an ideal password management system. This study likely provides insights into user preferences and requirements for such systems.

Overall, these works contribute to the understanding of password management system design, usability, security, and user perception.

In comparison to the referenced works on password management systems, our project takes a distinct approach by incorporating real-time password expiration alerts. While existing studies, such as "Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers" and "Privacy-Preserving Against Untrusted Browser Origins and Personalized Powerful Password Management," focus on enhancing effectiveness and privacy, our solution addresses the critical aspect of password security through timely reminders. By integrating password expiry tracking and alerts, our application ensures that users are promptly notified when their passwords are due for an update, thereby significantly reducing the risk of using outdated credentials.

In summary, our project amalgamates insights from these analyses to create a comprehensive and robust password management solution that emphasizes security, usability, and user satisfaction. While building upon existing research, we have strived to enhance the overall effectiveness and practicality of password management applications.

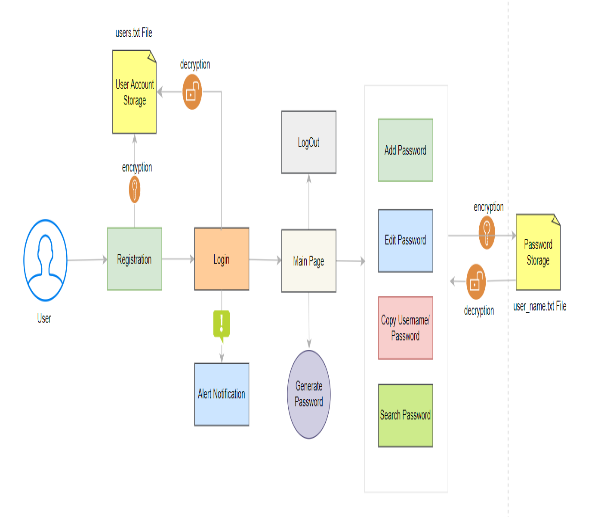
****

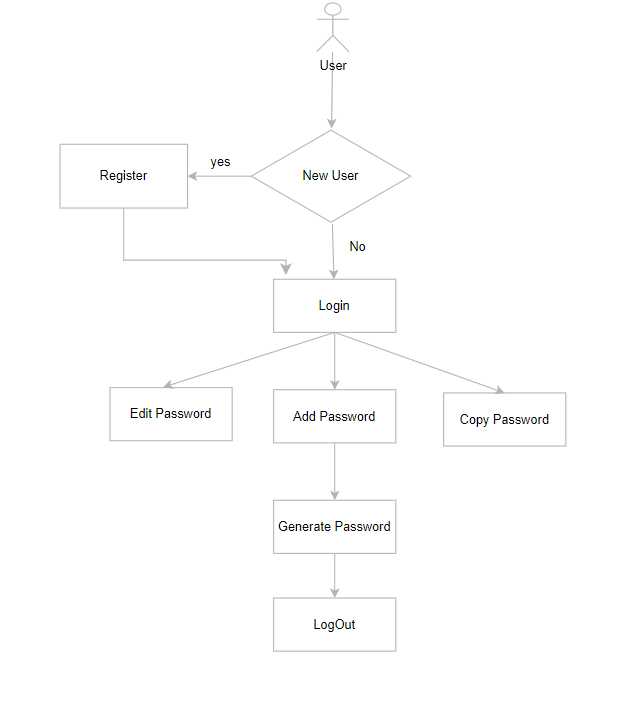
**Figure 1. Evaluation of popular PW Manager Software taken Table**

** Figure 2. Number of users and PW contains.**

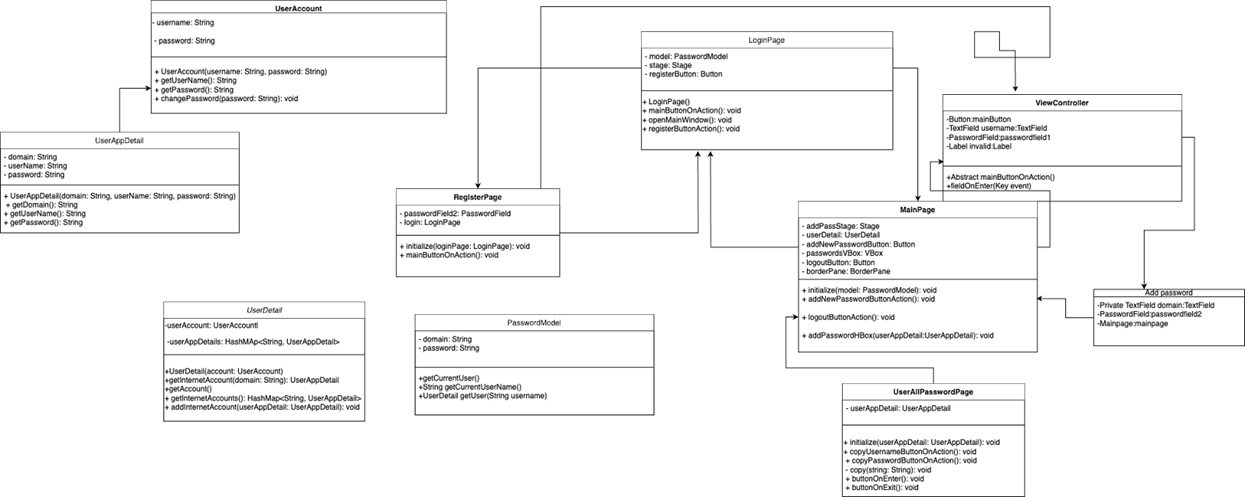
**Chart and table references taken from International Journal of Multidisciplinary and Current Research by Nooruldeen Nasih Qader**

**System Design:**

Here is the System Design of the Password Management System  
  
  
 **Figure 3. High-Level Design**



**Figure 4. UML Flow Diagram**

****

**Figure 5. UML Class Diagram**

**Implementation**:

**Architecture:**

•Utilized the Model-View-Controller (MVC) architectural pattern.

•Components: Controller, DAO (Data Access Object), and View.

•Followed Object Oriented Principles such as class Encapsulation, Inheritance, Polymorphism, Abstraction.

**Programming Language & Libraries:**

•Java as the primary programming language.

•JavaFX Library for building graphical user interfaces.

•Scene Builder to create UI layouts using FXML.

•Managed time-related operations using TimeUnit.

•Integrated AWT Toolkit and Clipboard for copying passwords.

•Utilized java.util.Date Library for handling time-sensitive operations

**Data Structures:**

•Utilized Collections, ArrayList and HashMap for efficient data storage and management.

**Password Generation and Encryption:**

•Generated secure passwords using SecureRandom and Base64.

•Implemented password encryption using Java's Cipher and SecretKey.

**Error Handling and Exception Management:**

•Implemented try-catch blocks to manage exceptions

•Handled FileNotFoundException and IOException

**Secure Key Generation:**

•Generated secure keys using KeyGenerator for encryption.

**User Interaction:**

•Created user interfaces using JavaFX and FXML

•Applied principles of Abstract Class and Inheritance for UI components

**File Handling and Data Management:**

•Handled IOException for file operations.

•Stored user data in files with proper error handling.

**Tools Used in the Project:**

•Eclipse

•Git repository

•Scene Builder

•Task Management Tools: Trello (<https://trello.com/>).

•Documentation Tools: Adobe Pdf, Google Docs, Google slide

•File (txt) for storage

**Data Persistence:**

•Implemented data persistence through File I/O operations.

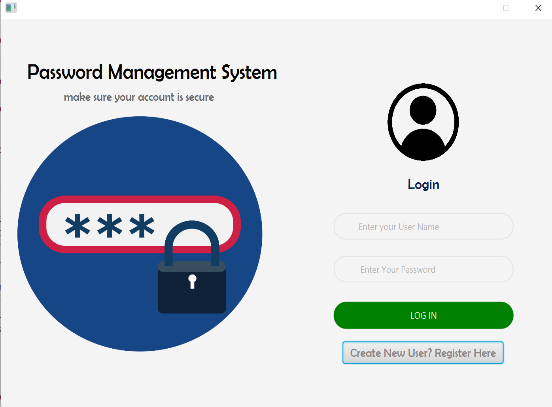
**Evaluation:**

Below are the screenshots showcasing the

different stages and functionalities of

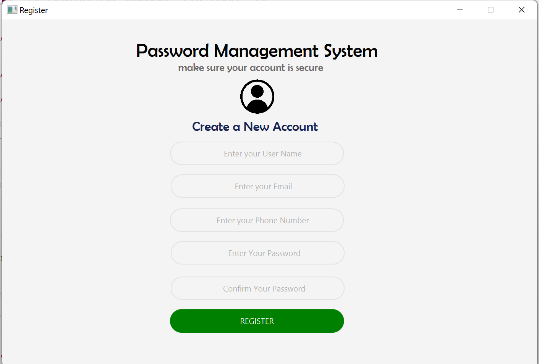
our application.

**Screenshot 1: Login Page**



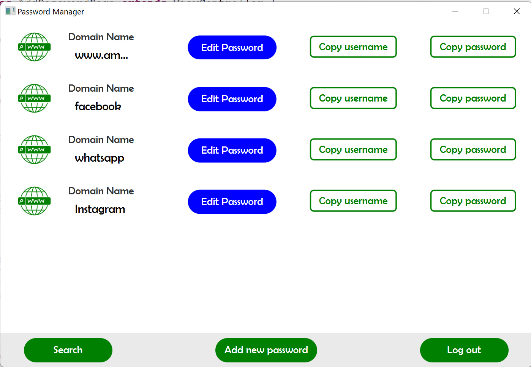
**Explanation:** Users start by logging into the application using their credentials.

**Screenshot 2: Register Page**



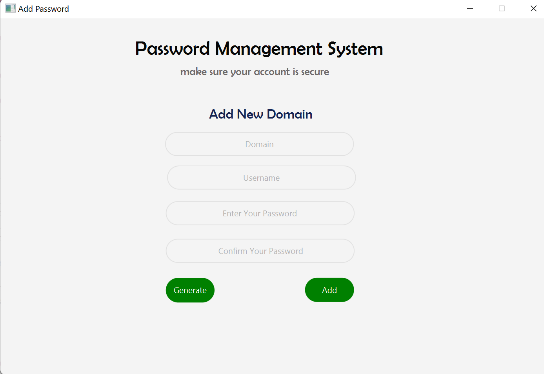
**Explanation:** If users don’t have an account, they can create a new account.

**Screenshot 3: Main Password Management Window**



**Explanation:** After logging in, users can access all the stored passwords with their details, where they can view, add, and edit passwords.

**Screenshot 4: Add New Password**



**Explanation:** Users can add a new password, including specifying a domain, username, and password.

**Screenshot 5: Edit and Update Password**

A screenshot of a computer

Description automatically generated

**Explanation**: Users can edit an existing password, update the information, and change passwords in the stored passwords.

**Screenshot 6: Generate Custom Password**

A screenshot of a computer

Description automatically generated

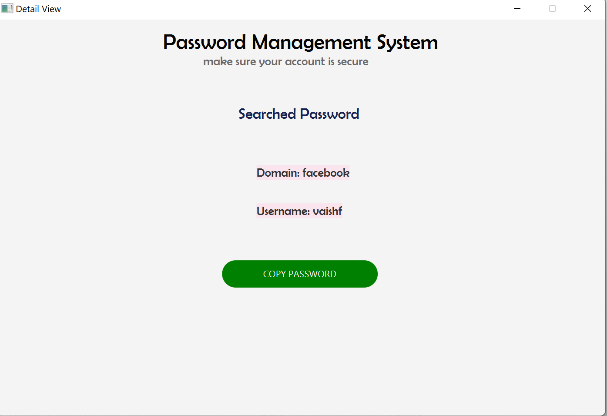
**Explanation**: Users can generate custom passwords that are more secure and have standard password criteria on Add Password Page.

**Screenshot 7: Search Password**.

Explanation: Users can search for passwords from the stored password to get fast and easy access to passwords.

A screenshot of a computer

Description automatically generated



**Discussion:**

In the implemented project, a comprehensive password manager application was developed to provide users with a secure and user-friendly environment for managing their passwords. The application enables users to store, edit, and organize their various online account credentials, promoting better security practices and minimizing the risks associated with weak or reused passwords. This discussion will delve into the various aspects of the project, highlighting its key features, contributions, challenges, and potential improvements.

The password manager application successfully fulfills the following key features:

1. User Authentication and Authorization:

2. Password Storage and Management:

3. Password Expiry and Alerts:

4. User-Friendly Interface:

**Contributions and Impact:**

The developed password manager application addresses a crucial need for robust password management in today's digital age. By providing users with a centralized and secure platform to store their credentials, the application contributes to improved cybersecurity practices. Users are empowered to create stronger passwords, avoid password reuse, and proactively update passwords as needed. This proactive approach to password security can significantly mitigate the risks of unauthorized access and data breaches.

In conclusion, the password manager project has successfully created an effective solution for users to manage their online account credentials securely. With further enhancements and refinements, the project can continue to evolve and play a significant role in promoting cybersecurity awareness and protection.

**Conclusion And Future Work:**

In this project, we successfully implemented a password management application that allows users to securely store and manage their internet account credentials. The application provides a user-friendly interface for adding, editing, and viewing passwords, enhancing user convenience and security.

**Advantages and Benefits:**

**1. User Authentication and Authorization:** Users are required to log in using their unique credentials, enhancing the security of their stored passwords. Password authentication is implemented to ensure that only authorized users can access their stored credentials.

**2. Password Storage and Management:** The application allows users to add, edit, and delete passwords for various online accounts. Passwords are securely stored using modern encryption techniques, protecting sensitive information from unauthorized access.

**3. Enhanced Security:** Our solution ensures that user passwords are securely stored and can be easily updated. The implementation of password expiration alerts adds an extra layer of security by prompting users to regularly update their passwords.

**4. Password Strength Evaluation:** Although the current implementation allows users to update passwords, an additional feature could include a password strength evaluation tool that guides users in creating stronger passwords.

**5. Password Expiry and Alerts:** The application offers a password expiry feature, allowing users to set expiration durations for their passwords. Users are notified through alerts when their passwords are due for expiration, promoting timely password updates and improved security.

**6. User-Friendly Interface:** The graphical user interface (GUI) provides a seamless and intuitive experience for users to interact with their stored passwords. Various functionalities, such as copying passwords to the clipboard, are easily accessible, streamlining the password management process.

**Problems and Future Work:**

**1. Browser:** Implementing Browser Extension that helps in easy and secure management of passwords on various websites

**2. Data Backup and Recovery**: Enabling regular data backups and providing a recovery option for lost passwords could prevent data loss and offer peace of mind to users.

**3. Auto-filling password:** Implementation of Auto-filling passwords can be measuring functionality which can save time and a convenient approach to securing passwords

If our team had more time, we would focus on implementing the above-mentioned improvements to elevate the security and usability of the password management application.

**Job Assignment:**

**Akansha Gupta:**

* + Password Encryption and Decryption implementation
  + Search Password Implementation
  + Generate Password Implementation
  + Alert Notification to change Password implementation
  + Copy Password Implementation
  + Add Password Implementation
  + Main Page Implementation
  + Error handling and exception management
  + High level Design
  + File Handling and Data Management
  + Maintained Version Control – Git
  + Prepared PPT and Report Document
  + Coordination with Mentor(TA) and Team
  + Team Code Review

**Vaishali Jeenwal:**

* + Implemented Base Project – Structured the project
  + UI Design for all pages
  + Register Page Implementation
  + Login Page Implementation
  + Edit Password Implementation
  + Add Password Implementation
  + Main Page Implementation
  + Error handling and exception management.
  + File Handling and Data Management
  + Maintained Version Control – Git
  + Prepared PPT and Report Document
  + Coordination with Mentor(TA) and Team
  + Team Code Review

**Akshitha Kamshetty:**

* + Password Strength analysis
  + Maintained Version Control – Git
  + Report Document
  + UML Diagram for System Design
  + Coordination with Mentor(TA) and Team
  + Team Code Review

**References:**

**Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers**

**By Quentin Stafford-Fraser**

https://www.academia.edu/48084224/Password\_Manager\_Friendly\_PMF\_Semantic\_Annotations\_to\_Improve\_the\_Effectiveness\_of\_Password\_Managers

**A Study for an Ideal Password Management System**

By Shivam K. Shinde, Mohit V. Deshpande

https://www.ijraset.com/research-paper/an-ideal-password-management-system

Privacy( Preserving( Against( Untrusted( Browser( Origins( and( Personalized( Powerful(

Password(Management

Privacy( Preserving( Against( Untrusted( Browser( Origins( and( Personalized( Powerful(

Password(Management

**Privacy-Preserving Against Untrusted Browser Origins and Personalized Powerful Password Management By Nooruldeen Nasih Qader**

https://www.researchgate.net/publication/262128075\_Privacy\_Preserving\_Against\_Untrusted\_Browser\_Origins\_and\_Personalized\_Powerful\_Password\_Management