Online Activity No. 8 and 9: Applying the User-Centered System Design Process

Chapter I. Introduction

Background of the study

Password management remains a significant challenge in 2025, as many users struggle to create and remember strong, unique passwords for the numerous online accounts they maintain. This often leads to weak or reused passwords, which increases the risk of unauthorized access and account breaches. Despite the advances in authentication technologies, such as biometrics and passkeys, passwords remain the primary method of login due to their widespread adoption. Cybercriminals exploit poor password habits through attacks such as phishing, brute force, and credential stuffing, making effective password management critical for digital security.

CYFER is a modern, secure, and user-friendly password manager designed to address these needs by providing encrypted vaults, intuitive interfaces, and seamless synchronization across devices, ensuring that users can store, manage, and retrieve their credentials safely and efficiently.

Statement of the problem

1. The existing password management systems often have complex and unintuitive user interfaces, causing users difficulty in efficiently storing and retrieving their credentials.
2. Many current password managers lack seamless synchronization across multiple devices, leading to inconsistent access and potential security risks when users switch between platforms.
3. Users frequently express concerns about privacy and data security due to insufficient encryption or unclear data handling policies in existing applications.
4. The absence of an integrated, user-friendly organizational system within password managers results in users struggling to categorize and manage numerous credentials effectively.
5. Some password managers have slow performance or time delays when searching for and retrieving stored passwords, negatively impacting user experience and productivity.

Assumption of the study

The CYFER password manager is designed to address the problems identified by incorporating the following features:

- A clean, intuitive, and user-friendly interface that simplifies the process of storing, retrieving, and managing passwords, reducing user frustration and errors.
- Robust end-to-end encryption protocols to ensure that all stored credentials remain private and secure, alleviating user concerns about data breaches.
- Seamless synchronization across multiple devices, guaranteeing consistent access to credentials regardless of platform or device used.

- An efficient organizational system that allows users to categorize and manage their credentials easily, improving navigation and retrieval speed.
- Optimized search functionality and performance enhancements to minimize delays in accessing stored passwords, thereby improving the overall user experience.

These features validate that CYFER's design sufficiently addresses the shortcomings of current password management systems, offering a secure, efficient, and user-centric solution.

Significance of the study

The proposed CYFER password manager benefits various stakeholders ranked from highest to lowest as follows:

- **Organizations' IT and Security Departments**
  CYFER enhances their ability to enforce strong password policies and secure credential management, reducing the risk of security breaches and simplifying compliance with data protection regulations.
- **Individual Users**
  The application provides a secure, easy-to-use platform for managing multiple passwords, reducing the likelihood of password reuse, and improving personal cybersecurity hygiene.
- **System Administrators**
  CYFER's seamless synchronization and centralized management features facilitate efficient oversight of user credentials across devices, streamlining administrative tasks.
- **Developers and UX Designers**
  The study offers insights into designing secure yet user-friendly applications, contributing to best practices in privacy-focused UX design1.
- **Organizations' Management Teams**
  By minimizing security incidents related to poor password management, CYFER supports business continuity and protects organizational reputation.

Each beneficiary gains specific advantages from CYFER's design, which prioritizes security, usability, and cross-device functionality, thereby supporting their respective roles effectively.

Chapter II. Research Design

This study employs the **User-Centered System Design (UCSD) Process**, an iterative approach that prioritizes understanding users, their tasks, and environments throughout all stages of design and development.

This section discusses the design process model used by the group wherein it is composed of the following stages:

A. Task Analysis

Hierarchical Task Analysis (HTA) was performed to break down the core tasks users perform with CYFER, focusing on the scope of password management. The main tasks include:

1. User Authentication
    a. Login to CYFER vault
    b. Multi-factor authentication (optional)
2. Password Management
    a. Add new credentials (username, password, URL)
    b. Edit existing credentials
    c. Delete credentials
3. Organizing Credentials
    a. Create categories or folders
    b. Move credentials between folders
4. Password Retrieval
    a. Search for credentials by keyword or category
    b. Copy or auto-fill passwords
5. Synchronization
    a. Sync vault data across devices
6. Settings and Security
    a. Change master password
    b. Enable biometric authentication
    c. Configure synchronization preferences

B. Requirements Gathering

The group employed multiple data gathering methods to collect comprehensive requirements:

- Interview
  Conducted interviews with potential users including individuals and IT professionals to understand pain points with existing password managers. Interviewees emphasized the need for simplicity, security, and cross-device access.
- Survey/Questionnaire
  Distributed questionnaires to a broader user base to quantify preferences on features such as encryption, synchronization, and interface design. This helped prioritize features like encrypted vaults and intuitive UI.
- Observation
  Observed users interacting with current password management tools to identify usability challenges such as complicated navigation and slow retrieval times.

User Requirements - Easy-to-use interface, fast retrieval, strong encryption, multi-device synchronization
Functional Requirements - Secure credential storage, search functionality, categorization, synchronization, backup

Data Requirements - Encrypted storage of passwords, secure transmission protocols
Environmental Requirements - Compatibility with Android and iOS devices, offline access capability
Usability Requirements - Intuitive navigation, minimal learning curve, accessible design for users with varying skills
Designer Requirements - Use of modern encryption standards, responsive design, scalable architecture

C. Storyboarding and Prototyping

Storyboarding: The team created storyboards illustrating typical user scenarios such as onboarding, adding a new password, searching for credentials, and syncing across devices. These visual narratives helped the team understand user flows and identify potential friction points early.
Prototyping:

- Developed low-fidelity wireframes to test layout and navigation.
- Progressed to high-fidelity interactive prototypes showcasing key features: vault creation, password entry forms, search bar, and synchronization settings.

User Manual Description:

- Input Forms: Users input credentials via simple forms with fields for website, username, password, and notes. Password strength indicators guide users during entry.
- Output: Credentials are displayed in categorized lists with search functionality. Users can copy passwords or use autofill features.
- Synchronization: Settings allow users to enable or disable cloud sync, with status indicators showing sync progress.
- Security Settings: Users can change master passwords and enable biometric login (fingerprint or face recognition).

D. Evaluation of prototype

Use heuristic evaluation with the format given below. These are the criteria for how the design will be graded.

Evaluation Criteria (Based on the 10 heuristics of design evaluation)

Area of Evaluation	5	4	3	2	1
A. Visibility of System Status – - The system design provides appropriate feedback like message prompts in response to user actions. – The message prompts are clear, visible and understandable.			X		
		X			
B. Match between the system and the real world - Used words, phrases and concepts according to users' language rather than system oriented words and computer jargons.		X			

C. User control and freedom - The system design provides ways of allowing users to easily "get in" and "get out" if they find themselves in unfamiliar parts of the system.		X			
D. Consistency and Standards – - The colors, text, labels, buttons and other elements in the design are uniform from start to finish**.**		X			
- Text and icons are not too small or too big.			X		
- Menus and other features of the system are arranged and positioned in a consistent way. (For ex. If your website has navigation buttons on the top under the page title on one page, the users will automatically look there for the same features on other pages.		X			
E. Error Prevention - The system design provides an automatic detection of errors and preventing them to occur in the first place.		X			
- Idiot proofing mechanisms are applied			X		
F. Help users recognize, diagnose and recover from errors **-** Error messages and the terms used are recognizable, familiar and understandable for the users.		X			
G. Recognition rather than recall **-** Objects, icons, actions and options are visible for the user. - Objects are labeled well with text and icons that can immediately be spotted by the user and matched with what they want to do.		X			
H. Flexibility and efficiency of use - The system design provides easy to navigate menus. - the system does not make wasteful time of system resources.		X			
I. Aesthetic and minimalist design **-**Graphics and animations used are not difficult to look at and does not clutter (mess) up the screen. - Information provided is relevant and needed for the system design.			X		
II. Help and Documentation **-**the system design provides information that can be easily searched and provides help in a set of concrete steps that can easily be followed.			X		

Chapter III. Conclusion and Recommendation

Conclusion

The CYFER password manager project addresses critical issues in secure and user-friendly credential management, aligning with the problems outlined in Chapter I. Existing systems often fall short in usability, security, or accessibility, leaving users vulnerable to poor password practices. CYFER bridges these gaps by offering an intuitive interface, robust end-to-end encryption, seamless synchronization across devices, and efficient organizational tools, thus enhancing both individual and organizational cybersecurity.

Specifically, CYFER tackles the problem of complex interfaces by providing a streamlined user experience, making it easier for users to store, retrieve, and manage their passwords. Its cross-device synchronization resolves inconsistencies and security risks associated with switching between platforms, while strong encryption protocols alleviate privacy concerns. The integrated organizational system and optimized search minimize the time and effort required to locate stored credentials, improving overall productivity.

Recommendations

To further enhance CYFER, the following recommendations are made:

- Continuous Security Audits: Regular security assessments and updates are essential to address emerging threats and maintain user trust.
- Enhanced Biometric Integration: Exploring integration with advanced biometric authentication methods, such as behavioral biometrics, could provide additional layers of security.
- Personalization Features: Implementing adaptive interfaces that tailor the user experience based on individual preferences and usage patterns could further improve usability.
- Expanding Platform Compatibility: Extending compatibility to emerging platforms, such as wearable devices and smart home systems, would broaden CYFER’s reach and convenience.

By prioritizing these ongoing improvements, CYFER can remain a leading password management solution, empowering users to protect their digital identities with confidence and ease.