Team No: 9

Sl.No	Student Name	Roll No
1	Adithya N S	CB.EN.U4CYS22002
2	Anaswara Suresh M K	CB.EN.U4CYS22007
3	C S Amritha	CB.EN.U4CYS22016
4	R.Sruthi	CB.EN.U4CYS22051

LockBox: A Secure Local Password Manager

Problem Statement

Most existing password managers are either too complex for everyday users or rely heavily on cloud storage, raising privacy concerns. There is a need for a secure, offline password manager that combines strong encryption with essential features like autofill, timeout lock, and an intuitive interface for easy navigation.

Scope and Relevance

- Most available tools are cloud-based (privacy concerns) or too complex for everyday users, leading to poor adoption.
- Modern cryptographic libraries and local storage capabilities make a secure offline solution realistic and efficient.
- Prioritizing both encryption and usability.
- A blend of offline security, autofill, timeout, and a user-first design, built for everyday use, not just tech-savvy users.

Suggestions and feedback from Last review

Date: 17th March 2025

Option Finalized :

- **Option 1:** Contribute directly to **KeePassXC**

- **Option 2:** Partially duplicate key features of **KeePassXC**
  → *We chose to proceed with Option 2*

1. Create a Feature List
2. Prioritize Features - Core (Must-Have), For Security, Extras (Optional Enhancements)
3. Reference Existing Tools - Analyze tools like **Bitwarden**
4. Platform Focus - Linux or Windows
5. **Phase I** – Build a basic, functional password manager with essential features only
6. **Phase II** – Add advanced features like **memory protection (RAM)**
7. Explore KeePassXC – Download and try the tool

Tools/Technologies Surveyed

KeePass is a lightweight local password manager mainly designed for Windows, with basic features, no cloud dependency, and limited cross-platform support.

KeePassXC is a privacy-focused password manager that stores all data locally, works entirely offline, and includes modern features like browser integration and TOTP.

Bitwarden is a cloud-based password manager that offers seamless syncing across devices, with optional self-hosting.

Google Password Manager is a built-in cloud service that saves and autofills passwords across Chrome and Android, tightly integrated with your Google account.

Comparison of tools

KeePass	KeePassXC	Bitwarden	Google Password Manager
KeePass for Windows, built on .NET with a simple, secure local password storage.	A cross-platform KeePass variant (C++/Qt).	Cloud-based password manager with self-hosting option	Built into Chrome/Android, syncs via Google account.
Fully offline	Fully offline	Needs setup	Cloud-only
Windows-only	Windows /Linux / macOS	Web/Desktop/Mobile	Chrome, Android, iOS
Supports lockout timers and clipboard wiping	Supports lockout timers and clipboard wiping	Supports memory hardening , lockout timers and clipboard wiping	Doesn't support memory hardening, lockout timers and clipboard wiping
Uses AES-256 + PBKDF2 for Encryption	Uses AES-256 + Argon2 Encryption	Uses AES-256 + PBKDF2 Encryption	Encrypted managed by Google

Paper Analyzed: "Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions" (2025)
Authors: Petr Gallus, Dominik Staněk, Ivo Klaban

Key highlights:

- **Top 3 Most Secure Password Managers**
  a. Bitwarden (100% security score)
  b. 1Password (99% security score)
  c. ProtonPass (98% security score)
- **Critical Security Issues Found**
  a. Some password managers leave passwords visible in memory
  b. KeePass lacks phishing protection - manual URL verification required
- Effective password managers implement URL matching and detection mechanisms to prevent credential autofill on suspicious or phishing websites.

Progress made since second review

Mandatory Features:

- Master Password
- Encrypted Database
- Password Generator
- Auto Lock Timeout
- Search Functionality
- Local Storage
- Autofill

Additional Features:

- Two - factor Authentication
- Cross Platform
- check with Have I been Pwned

Paper Analyzed: Vault-PMS: A Vault-Based Password Management System for Secure Offline Data Storage (2024)
Authors: UAE University Research Team

Key highlights:

1. The triple-layer approach (AES-256 + MFA + Backup) provides a solid foundation
2. Modular design with separate classes for different functions
3. Clear limitations in user experience, browser integration, and cross-platform support
4. Key enhancement areas identified - modern UI/UX design and seamless browser auto-fill integration - providing a clear roadmap to combine Vault-PMS security foundations with superior user experience features

Paper Analyzed: Analysis on the Security and Use of Password Managers
Authors: Carlos Luevanos, John Elizarraras, Khai Hirschi, Jyh-haw Yeh

Key highlights:

1. Most tools (except Padlock) default to cloud/server storage, increasing exposure to breaches. The paper notes Encryptr's cloud reliance as a risk.
2. None of the open-source managers effectively implement secure auto-fill, leaving users vulnerable to clipboard/key-logger attacks.
3. Open-source tools often lack intuitive interfaces, while closed-source tools obscure security practices.
4. Padlock's weak default password generator contradicts NIST standards, highlighting inconsistent enforcement.

Reference

- Gallus, P., Staněk, D., & Klaban, I. (2025). *Security evaluation of password managers: A comparative analysis and penetration testing of existing solutions*. In Proceedings of the 20th International Conference on Cyber Warfare and Security, ICCWS 2025 (pp. 105-113). University of Defence.
- Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J.-H. (2017). *Analysis on the security and use of password managers*. 2017 IEEE Conference on Privacy, Security, and Cryptography (PSC).
- Baskar, K., Muthumanickam, K., Vijayalakshmi, P., & Kumarganesh, S. (2024). A Strong Password Manager Using Multiple Encryption Techniques. *Journal of the Institution of Engineers (India) Series B*. https://doi.org/10.1007/s40031-024-01144-6
- Abdulkadir, M., Alketbi, S., Lamaazi, H., Altamimi, R., Alblooshi, S., & Lakas, A. (2024). *Vault-PMS: A vault-based password management system for secure offline data storage. In 2024* International Wireless Communications and Mobile Computing (IWCMC) (pp. 1510-1515). IEEE.
- https://github.com/keepassxreboot/keepassxc/wiki
- https://github.com/bitwarden