Group Number : 09

# Lock Box - Offline Password Manager

**Domain:** Cybersecurity & Data Protection
**Guide Name:** Dr. C Srinivasan
**Date:** 15-09-2025

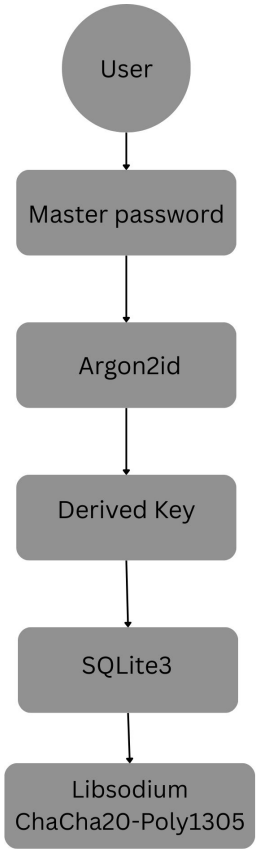
| Sl.No | Student Name | Roll No |
|---|---|---|
| 1 | Adithya N S | CB.EN.U4CYS22002 |
| 2 | Anaswara Suresh M K | CB.EN.U4CYS22007 |
| 3 | C S Amritha | CB.EN.U4CYS22016 |
| 4 | R Sruthi | CB.EN.U4CYS22051 |

## Problem Statement Recap

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.

# Architecture Diagram

- When the user enters their master password, the **Argon2id** key derivation function is used to generate a unique encryption key.
- This derived key is then used with the **ChaCha20-Poly1305** encryption algorithm from the **libsodium** library to encrypt the entire SQLite database file.



# Phase 2: Core Development (September - October 2025)

## Month 3: September 2025 - Encryption Module

- encryption/decryption module implementation
- Secure random number generation for passwords and salts
- Key derivation function implementation
- SQLite database creation with encryption layer
- Master password validation system implementation
- Encrypted credential storage and retrieval functions
- Basic database operations for password entries

## Month 4: October 2025 - User Interface & Basic Features

- Main application window with login interface
- Credential management interface (add/edit/delete passwords)
- Basic search functionality implementation
- Auto-lock timeout mechanism
- Password strength analyzer and duplicate detection
- Local storage management and backup functionality
- First demo preparation and testing

# References


- https://github.com/bitwarden/desktop
- https://github.com/bitwarden/clients
- https://bitwarden.com/help/what-encryption-is-used/
- https://github.com/keepassxreboot/keepassxc
- https://scythe-studio.com/en/blog/4-best-frameworks-for-cross-platform-desktop-app-development
- https://medium.com/@pravallikayakkala123/understanding-aes-encryption-and-aes-gcm-mode-an-in-depth-exploration-using-java-e03be85a3faa
- https://github.com/alexedwards/argon2id
- https://github.com/jedisct1/libsodium
- https://www.canva.com/design/DAGyyeCxvmQ/nTYp8NUycby9kWokqk1PiQ/edit?utm_content=DAGyyeCxvmQ&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton
- https://libsodium.gitbook.io/doc/secret-key_cryptography/aead/chacha20-poly1305/original_chacha20-poly1305_construction