

# Project 2: CLI Password Manager

K. Sandeep kumar

# Introduction

- This project is a secure command-line password manager.
- It stores website credentials with AES-256 encryption.
- All data stays safe using a master password system.

# Features

- Add new credentials
- Retrieve saved passwords
- List all stored sites
- Delete entries
- Works with hidden password prompts

# Security

- AES-256 encryption for strong protection
- Master password with PBKDF2 key derivation
- Authenticated encryption with AES-GCM
- Brute-force protection with lockouts






# Data Storage

- Encrypted data saved in JSON file (vault.json)
- Metadata stored (salt, nonce, authentication tag)
- Atomic writes prevent data corruption

# Responsibilities

1. CLI design with argparse
2. Cryptographic security (AES, PBKDF2)
3. JSON-based storage
4. Master password authentication
5. Error handling & validation

# Skills Gained

-  CLI design with argparse
-  Cryptographic security knowledge
-  Secure JSON data storage
-  Error handling & validation
-  Defense against attacks

# Learning Outcomes

- Build secure CLI applications
- Work with encryption & decryption
- Design safe data storage systems
- Learn cryptography best practices
- Handle sensitive data responsibly