National University of Computer & Emerging Sciences

Karachi Campus

Password Managing Application

Project Proposal

Cyber Security

Section: CY-A

Group Members:

23K-2005 Muhammad Hammad

23K-2031 Muhammad Sami Ashfaq

Professor:

Mr. Fahad Samad

Project Proposal

- **Introduction:**

In today's digital age, users often need to remember numerous passwords for various platforms and services. Manually managing and recalling these passwords can lead to security vulnerabilities, such as reusing weak passwords or writing them down. A password manager can solve these issues by securely storing passwords, allowing users to retrieve them efficiently while ensuring protection through encryption.

- **Existing System:**

Currently, many users rely on manual methods of storing their passwords, such as using spreadsheets, physical notes, or relying on memory. Alternatively, some users opt for third-party password managers, but they often involve a subscription or lack transparency in security practices. Additionally, users may have concerns about trusting their sensitive information with these services.

- **Problem Statement:**

Managing multiple, complex passwords has become increasingly challenging for users. Without a reliable password management solution, users are prone to adopting insecure practices such as password reuse, using weak passwords, or storing them unsafely. These practices increase the risk of account compromise and data breaches, leading to unauthorized access and financial losses.

- **Proposed Solution:**

Our project aims to develop a secure desktop-based password manager application that allows users to store, retrieve, and manage their passwords easily. The application will incorporate encryption techniques to ensure that stored passwords remain confidential and protected from unauthorized access. By providing a user-friendly interface, this tool will encourage secure password management practices.

- ## Salient Features:

Password Storage: Securely store passwords using strong encryption methods.

Password Retrieval: Allow users to retrieve stored passwords using a master password or other authentication methods.

Encryption: All passwords will be encrypted to ensure confidentiality and data integrity.

Cross-Platform Compatibility: The app will be built for Windows but could be extended to support other operating systems in the future.

User-Friendly Interface: A simple and intuitive interface for ease of use.

- ## Tools & Technologies:

Programming Language: C++ or Python

Framework: None

Operating System: Windows