Synopsis On

Password Manager

For Term 1 Project

Subject- Computer Science ( Python )

Academic Year ( 2021 - 22 )

Submitted To- Submitted By-

Ms

Introduction:

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database, or calculating them on demand.

# Problem Statement:

Passwords are a ubiquitous part of the digital age. They are the keys to unlocking our online profiles that are hosted across a plethora of websites. With each of our profiles necessitating a separate password, it is not uncommon for people to need up to 50 passwords.

It is therefore unsurprising that the worst passwords of 2015, as revealed by TeamsID earlier this year, remained “123456”, “password”, “12345678” and “qwerty”. This is despite continuous advice and education to the contrary, as security gives way to convenience.

Recent events have now seen hundreds of millions of passwords leaked online, when more than one hundred million LinkedIn logins and tens of millions of Twitter logins were made available on the darknet.

The problem with passwords is that, for them to be effective, they need to be an uncommon word, of eight letters or more and not used anywhere else. However, memorising fifty or more passwords is difficult, to say the least. “It is very difficult to have complex and unique passwords for as many sites as required,” says security advisor Sean Sullivan of F-Secure. “It is understandable [that people reuse them] because they are required to use so many passwords.

# Objective:

To create a GUI based password manager which is easy to use and intuitive. This Program should help out every one to organise their there passwords.

# The advantages of the proposed system are:

The advantage of password-based access controls is that they are easily incorporated in most software using APIs available in many software products, they require no extensive computer/server modifications, and that users are already familiar with the use of passwords. While passwords can be fairly secure, the weakness is how users choose and manage them, by using:

* simple passwords – short in length, that use words found in dictionaries, or do not mix in different character types (numbers, punctuation, upper/lower case), or are otherwise easily guessable
* passwords others can find – on sticky notes on monitors, in a notepad by the computer, in a document on the computer, whiteboard reminders, smart device storage in clear text, etc.
* the same password – using the same password for multiple sites, never changing account passwords, etc.
* shared passwords – users telling others passwords, sending unencrypted emails with password information, contractors using same password for all their accounts, etc.
* administrative account logins where limited logins would suffice, or
* administrators who allow users with the same role to use the same password.

# Contribution in real world

To avoid Password Fatigue

Aside from contributing to stress, password fatigue may encourage people to adopt habits that reduce the security of their protected information. For example, an account holder might use the same password for several different accounts, deliberately choose easy-to-remember passwords that are too vulnerable to cracking, or rely on written records of their passwords.

According to a survey conducted in February 2020 by password manager Nordpass, a typical user has 100 passwords

Our proposed program aims to simplify Password Keeping and avoid aforementioned password fatigue