PASSWORD MANAGER WITH SMART RECOVERY

MUHAMMAD AMIRUL NAJMI BIN MOHD FADZIL

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: **PASSWORD MANAGER WITH SMART RECOVERY**

SESI PENGAJIAN: 2022/2023

Saya: MUHAMMAD AMIRUL NAJMI BIN MOHD FADZIL

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
✓	TIDAK TERHAD	

(TANDATANGAN PELAJAR)	(TANDATANGAN PENYELIA)
Alamat tetap: 1885 MUKIM 9, TANAH LIAT, 14000 BUKIT MERTAJAM, PULAU PINANG	MRS. KHADIJAH BINTI WAN MOHD GHAZALI
Tarikh: 23 SEPTEMBER 2023	Tarikh: 23 SEPTEMBER 2023

PASSWORD MANAGER WITH SMART RECOVERY

MUHAMMAD AMIRUL NAJMI BIN MOHD FADZIL

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

PASSWORD MANAGER WITH SMART RECOVERY

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 20 September 2023
(MUHAMMAD AMIRUL NAJMI BIN MOHD FADZIL)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Security) with Honours.

SUPERVISOR : Khadijah Date : 20 September 2023
(MRS. KHADIJAH BINTI WAN MOHD GHAZALI)

DEDICATION

Dedicated to all those who have embarked on the journey of knowledge, innovation, and software development. This project report is a tribute to the countless hours of learning, designing, coding, and testing that have been invested. It is a testament to the unyielding determination and resilience in overcoming challenges and seeking solutions.

To our mentors and educators, thank you for guiding us and igniting our passion for computer science. To our friends and families, thank you for your unwavering support and encouragement throughout this endeavor. And to our team members and collaborators, thank you for your dedication, collaboration, and shared vision that has shaped this software development project.

May this report inspire and contribute to the ever-evolving field of computer science, paving the way for future innovations and advancements.

ACKNOWLEDGEMENTS

I want to openly thank and appreciate everyone who has assisted me. who have helped this final year project report in computer science software development to be completed successfully.

From the beginning, I would like to express my deepest appreciation to my project supervisor, MRS. KHADIJAH BINTI WAN MOHD GHAZALI whose counsel, expertise, and unwavering support have been indispensable throughout this process. Their constructive criticism, tolerance, and support have helped me shape my work and increase my understanding. I'm also thankful to my family and friends for always being there for me and cheering me on during this final year project.

I thank all the researchers, writers, and developers whose work and open-source contributions inspired this project. The project's ideas and implementation plans were greatly aided by the online resources.

Finally, I am grateful to everyone who helped complete my final year project. I'm grateful to have worked on this software development project with your help, instruction, and encouragement.

ABSTRACT

The project titled "Password Manager with Smart Recovery" proposes the creation of an innovative password manager that addresses the issues of secure password management in the complicated digital ecosystem of today. The goal of this project is to develop a system that not only provides users with the ability to safely store and organize their passwords but also incorporates user recovery features. The phases involved in this development work using Agile Methodology that include some step that are analysis of existing works, followed by requirement analysis for the project, designing the system, developing the code, and followed by implementation and testing. After all the steps are completed, the system is ready to be deployed. The project will result in a secure and convenient password manager that allows users to store and manage their passwords securely, and to make sure that their loved ones can access them if they pass away. The password manager will use a decentralized architecture, strong encryption for password by using AES encryption, multi-factor authentication, and smart recovery features. This project represents a significant advancement in password management solutions, offering both enhanced security and user convenience.

ABSTRAK

Projek bertajuk "Pengurus Kata Laluan dengan Pemulihan Pintar" mencadangkan penciptaan sebuah pengurus kata laluan inovatif yang mengatasi isu-isu pengurusan kata laluan yang selamat dalam ekosistem digital yang rumit pada masa kini. Matlamat projek ini adalah untuk membangunkan sistem yang tidak hanya memberi pengguna keupayaan untuk menyimpan dan mengatur kata laluan pengguna dengan selamat, tetapi juga menyertakan ciri pemulihan pengguna. Fasa-fasa yang terlibat dalam pembangunan ini menggunakan Metodologi Agile yang merangkumi beberapa langkah yang termasuk analisis kerja sedia ada, diikuti dengan analisis keperluan untuk projek, merancang sistem, mengembangkan kod, dan diikuti dengan pelaksanaan dan pengujian. Setelah semua langkah selesai, sistem ini bersedia untuk diterapkan. Projek ini akan menghasilkan pengurus kata laluan yang selamat dan mudah digunakan yang membolehkan pengguna menyimpan dan mengurus kata laluan mereka dengan selamat, dan memastikan bahawa orang tersayang mereka dapat mengaksesnya jika mereka meninggal dunia. Pengurus kata laluan ini akan menggunakan senibina terdesentralisasi, penyulitan yang kuat untuk kata laluan dengan menggunakan penyulitan AES, autentikasi pelbagai faktor, dan ciri pemulihan pintar. Projek ini mewakili kemajuan yang signifikan dalam penyelesaian pengurusan kata laluan, menawarkan keselamatan yang ditingkatkan dan keselesaan pengguna.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

CHAPTER 1: INTRODUCTION

1.1 Introduction

A password manager is software that allows users to securely store and manage passwords across multiple websites and accounts. It allows users to establish complicated and unique passwords for each account and saves them in an encrypted format that the user may only access with a master password.

In today's digital world, where people have multiple online accounts, remembering unique passwords for each one might be difficult. Using the same password for many accounts is a serious security risk because a data breach on one account could potentially expose all other accounts that use the same password.

As a result, a password manager is a beneficial tool that can help users simplify password management, improve security, and reduce time. It can also generate unique and random passwords, autofill login forms, and have two-factor authentication.

This project involves building a password manager that not only stores passwords but also provides a mechanism for deceased user recovery. This feature allows the user to designate a trusted person, such as a family member or executor, who can request access to the user's accounts after they pass away. Creating a password manager with deceased user recovery capabilities is challenging but worthwhile taking on that can benefit users and their loved ones. It can ease some of the stress and uncertainty associated with managing digital assets after someone dies.

1.2 Problem Statement

The problem that has been identified is summarized in Table 1.1 below.

Table 1.1 Problem Statement

PS	Problem Statement
PS1	Passwords are hard to remember, and users often have multiple accounts that require passwords. As a result, users choose memorable but poor passwords and then overuse them, causing serious security issues.
PS2	potential loss of access to important online accounts and digital assets due to the user's death. Many people do not have a designated person who has access to their account information, which makes it difficult for their loved ones to recover these assets.

1.3 Problem Question

According to the problem statement above, the following questions are set up.

Table 1.2 Problem Question

PS	PQ	Problem Question
PS1	**PQ1**	How can the password manager ensure that users create strong and unique passwords for their accounts?
	PQ2	What measures can the password manager take to prevent users from overusing the same password across multiple accounts?
PS2	**PQ1**	How the user account and password will be after the user death and how to pass the user account to the family member or trusted contact after user death?

1.4 Project Objective

Based on the project questions formulated in previous section, appropriate project objectives (PO) are developed as follows. The Project Objectives (PO) is summarized into Table 1.3 below.

Table 1.3 Project Objective

PS	PQ	PO	Project Objective
PS1	**PQ1**	**PO1**	Develop a password strength meter that provides real-time feedback to users on the strength of their passwords and encourages them to create unique and strong passwords for each of their accounts.
	PQ2	**PO2**	Develop a Multi factor authentication include email verification and security code for login and registration to ensure security to the user account.
PS2	**PQ1**	**PO1**	Develop recovery mechanism in event of user death to help their family or trusted person to have access to their account for accessing the user password.

1.5 Project Scope

The Scope of this project is going to handle as follows:

1. To enable users to securely store and manage their passwords and account information in a centralized platform, while also offering convenient features like password strength meter, password generator and two-factor authentication.
2. To Include a smart deceased user recovery system that allows users to designate a trusted person who will be able to access their account information in the event of their death.

1.6 Project Contribution

The contribution of this project is summarized in Table 1.4

Table 1.4 Project Contribution

PS	PQ	PO	PC	Project Contribution
PS1	**PQ1**	**PO1**	**PC1**	Develop an accurate and reliable password strength meter algorithm tailored to the password manager's specific needs, which provides real-time feedback to users on the strength of their passwords and encourages them to create strong and unique passwords for each account.
	PQ2	**PO2**	**PC2**	Develop a Multi factor authentication to ensure security to the user account based on the user preferences.
PS2	**PQ1**	**PO1**	**PC1**	Develop a secure recovery process that allows users to pass on their account information to designated beneficiaries after death, while also implementing a robust verification process that uses multiple identification forms to verify account access requests.

1.7 Report Organisation

Chapter 1: Introductions

Provides an overview of the project's objectives, scope, and significance.

Chapter 2: Literature Review

Present related work and research, including exploration of other applications, database connectivity and system operation.

Chapter 3: Project Methodology

Describe the approach used to complete the project, detailing the various phases and actions taken.

Chapter 4: Design

Explores problem and requirement analysis, with a focus on high-level design, user interface design and system architecture.

Chapter 5: Implementation

Outlines the activities involved in the implementation phase, including software development environment setup, software configuration management, and current implementation status.

Chapter 6: Testing & Analysis

Examines the testing phase, including the test plan, test environment, test schedule and test strategy, as well as the results and analysis.

Chapter 7: Conclusion

Summarizes the project, including how the objectives were achieved, the strengths and weaknesses, and the project’s contributions.

1.8 Conclusion

This his introductory chapter offers an overview of the entire project, including the problem statement, project question, project objective, and scope. It highlights the improvements made to the Password Manager with Deceased User function. The subsequent chapter, the literature review, will delve into further details about Password Manager with Smart Recovery.

CHAPTER 2: LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter will discuss the literature review using examples from related published information and materials such as articles, websites, journals, and published papers. This chapter will help in the study of concepts, problems, procedures, methodologies, and research patterns for this project derived from previous projects. To accomplish the project's objectives, a better knowledge of the concept and technique must be clear so that it can be accomplished more easily.

2.2 Domain

The domain on this system focuses on storing and protect the passwords used by individuals or organizations to protect their accounts and sensitive information in a safe place.

2.3 Facts and findings

2.3.1 Password

A password is a sequence of characters that provides authorization for entry into a computer system or an online account (Wikipedia, 2019).

2.3.2 Password Manager

A password manager is a software or tool that stores and manages passwords for user in a safe place (Vultur, 2016).

2.3.3 Authentication

Authentication is a process when user provides his identity to the system when logging in.

2.3.4 Authentication factor

Refer to an information verification method used to confirm the user identity for example user confirm their provided images.

2.3.5 Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is using various factors, such as knowledge or biometrics. It functions to authenticate a user, increasing the security while preventing unauthorized access.

2.3.6 Autofill

Autofill is a feature that will automatically fill form fields with stored data that can save time and effort for users.

2.3.7 Password Encryption

process of converting user password into a safe and unreadable format through cryptographic algorithms to prevent unauthorized access.

2.3.8 Deceased User Smart Recovery

refers to a feature or mechanism that was created to deal with the situation when a password manager user dies and their stored passwords need to be recovered or accessed by authorized individuals, like family members.