

# WEB BASED PASSWORD MANAGEMENT SYSTEM

CHAVALIT A/L TAT WI

Thesis submitted in fulfilment of the requirements  
for the award of the degree of  
Bachelor of Computer Science (Software Engineering)

Faculty of Computer Systems & Software Engineering  
UNIVERSITI MALAYSIA PAHANG

JUNE 2017

### **STUDENT'S DECLARATION**

I hereby declare that the work in his thesis entitled “WEB BASED PASSWORD MANAGEMENT SYSTEM” is my own except for quotations and summaries which have been fully acknowledged.

Signature :

Name : CHAVALIT A/L TAT WI

ID Number : CB14144

Date :

## **SUPERVISOR'S DECLARATION**

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Software Engineering).

Signature :

Name : DR ERIC LIEW SIAU CHUIN

Date :

## TABLE OF CONTENTS

CONTENT	Page
<b>LIST OF TABLES</b>	iii
<b>LIST OF FIGURES</b>	iv
<b>LIST OF ABBREVIATIONS</b>	v
<b>CHAPTER 1          INTRODUCTION</b>	
1.1                    INTRODUCTION	1
1.2                    PROBLEM STATEMENT	2
1.3                    OBJECTIVE	2
1.4                    SCOPE	3
1.5                    THESIS ORGANIZATION	4
<b>CHAPTER 2          LITERATURE REVIEW</b>	
2.1                    INTRODUCTION	5
2.2                    EXISTING SYSTEM	7
2.2.1    Clipperz	7
2.2.2    Passpack	8
2.2.3    MyPadLock	9
2.2.4    Comparison between existing systems	10

**CHAPTER 3                      METHODOLOGY**

3.1	INTRODUCTION	11
3.2	METHODOLOGY	12
	3.2.1 Justification of Chosen Methodology	12
	3.2.2 Context diagram	14
	3.2.3 Software Requirement Specification (SRS)	14
	3.2.4 Software Design Document (SDD)	14
	3.2.5 Use Case Diagram	15
	3.2.6 Modules of System	16
	3.2.7 Dialogue Diagram	18
3.3	HARDWARE AND SOFTWARE REQUIREMENT	
	3.3.1 Hardware Requirement	19
	3.3.2 Software Requirement	19
3.4	GANTT CHART	20
3.5	IMPLEMENTATION	21
3.6	TESTING	23

**REFERENCES****APPENDICES**

**LIST OF TABLES**

<b>Table No.</b>	<b>Title</b>	<b>Page</b>
2.1	Advantages and Disadvantages of Clipperz	7
2.2	Advantages and Disadvantages of Passpack	8
2.3	Advantages and Disadvantages of MyPadLock	9
2.4	Comparison of Three Existing Systems	10
3.1	Hardware Tools used in development	19
3.2	Software Tools used in development	19

**LIST OF FIGURES**

<b>Figure No</b>	<b>Title</b>	<b>Page</b>
2.1	Clipperz system	7
2.2	Passpack system	8
2.3	MyPadLock system	9
3.1	RAD model	12
3.2	Context diagram	14
3.3	Use case diagram	15
3.4	Package diagram	16
3.5	Dialogue diagram	18
3.6	Gantt Chart	20

## **LIST OF ABBREVIATION**

CSS	Cascading Style Sheets
HTML	HyperText Markup Language
IDE	Integrated Development Environment
PHP	PHP: Hypertext Preprocessor
SQL	Structured Query Language
AES	Advanced Encryption Standard



## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 INTRODUCTION**

Security of users and privacy often become a big issue in the virtual world. Normal users' use online services which social media sites, blogging, video or music streaming sites, online shopping marts. Users at work use work emails and account for business purposes.

A casual user uses many online services online. Users are given account to access services. Common sites for a user are email services which are Google, Yahoo or user login to their company email accounts. The registration includes the services asking the new user to fill some information such as name, age, email, username and password and other related information. After registration finishes, an email is sent where their account is verified after click an appropriate links.

Next, they will redirect to the main page or login page of the system. They will ask the user to insert username or email, and password so that they can login to their accounts. Now, they have full authority of the account of the online services that they can use.

Web Based Password Management System is a web-based management system where a user can store private information which as passwords so that they can keep tracks of the different password which are login information for any websites, applications or devices that they used in daily life. When the user keeps an

account online, this means they trust their privacy when using the online services. Therefore, the password should be secure, long and unbreakable by hackers.

The web-based management system is built on text editors which are Notepad++ and any web browser such as Mozilla Firefox, Google Chrome, and Internet Explorer. The languages used are HTML, CSS, JavaScript and PHP while database language use for storing information is SQL.

## **1.2 PROBLEM STATEMENT**

The first problems that can be addressed are that users have many accounts for same online services and vice versa. This produce confusions as some users have trouble remembering many accounts and password. These create hassles as users need to access their preferred services at a short time. Normal online services will prompt the user to fill in their username or email so they can send temporary password so that can login. After they log in, they will change the temporary password and go through steps which are bothersome. Therefore, the problems can be solved if users know which password for which accounts and able to distinguish between each service they used.

Second major problems are that users don't have a specific and secure place to store private information. People usually wrote private information such as passwords inside a diary, notebook, sticky notes, and stickers on the computer peripherals which are keyboard and monitor. Password are being written in obvious places where can be easily seen by other people. We can see where unwanted scenario, if the diary, notes are missing or stolen by people, this will cause trouble to users. This is dangerous as other people who are close to them or unwanted parties that gain access and doing criminal activities, scams, phishing, and cyber bullying using their accounts. The solution would be that a platform where users don't have to write the password on physical items such as notebooks or on sticky notes. At the

same time, they can carry password manager which are assessable at any time and any place.

The third issue can be discussed are password strength that created by users. The weakness of the passwords that is an issue which is predictable, short and containing related information about users. Another party can repeat guessing and able to break into accounts at a short time where they can misuse their accounts. Some users their own name, birthday date, age, names of their personal belonging or beloved ones as password which can be easily predicted or guess by another party. There must be password checker and strength evaluation so that user will able to have a secure password.

### **1.3 OBJECTIVES**

The main purposes of the project are;

- i. To investigate the current password management system.
- ii. To propose web based system that can store private information securely mainly password information.
- iii. To evaluate the proposed system.

### **1.4 SCOPE**

The main scopes of project are;

- i. The user that uses any online services and offline services which are websites, applications, and devices that require a password as an authentication before using them.
- ii. The user which understands the English language or any language and have good computer literacy in using websites, applications, and devices.
- iii. The password management system is built using web-based programming languages which can be viewable using a web browser.

## **1.5 THESIS ORGANIZATION**

This thesis consists three chapters from Chapter 1: Introduction, Chapter 2: Literature Review and Chapter 3: Methodology. Firstly, the first chapter discusses on introduction, problem statement, objective, scope and thesis organization. Next, second chapter discusses on current existing systems and comparison between three existing systems for analysis. The final chapter of thesis is on methodology, selected methodology for development, context diagram, use case diagram, modules, hardware and software requirements, Gantt chart, implementation and testing methods.

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1 INTRODUCTION**

The web password management system is a system that store password and related private information at one place. The web-based password management is built using web programming language which are HTML, CSS, PHP and database query language which are SQL.

A web-based system is chosen as a solution due to its ability to be deployed in various types of browser environments, computers, devices as tablets and smartphone. Many website that is built can be viewed in various web browsers such as Mozilla Firefox, Google Chrome, Internet Explorer or Microsoft Edge, Safari and other browsers. This makes the web based system can be easily accessible across different type of devices.

A web-based system cost is usually effective. This is due the nature of developers doesn't have to invest Integrated Development Environment which IDE that has all premium features for different programming languages such as C#,VB.Net and other tools that can help the software development such Visual Studio Professional for developing systems. A developer doesn't need to install many various tools, drivers, software packages, undergone testing and encounter many errors like other programming languages in order to run properly such as C programming and VB.Net that requires a user to run an executable file without errors.

A web-based system can be built by inserting HTML, CSS, PHP, and SQL code inside a Notepad file which the extensions can be changed easily. There are many free development tools for web programming and scripting languages such as Notepad++, Netbeans IDE, Visual Studio Code. There are also payable tools such as Adobe Dreamweaver can be viewed as great optional development area due to its simplicity in offering drag and drop features for designing websites. In this era, we can see many different types of web applications that can be viewed as hybrid as it can be the combination of both mobile development and web development so developers have many solutions for different problems.

A web-based system can be easily maintained by developers. This is because developers can be maintained the code in a different environment, integrated software development, operating systems or inside a content management systems. A SQL language has many advantages as it can store inside a web server or in a standalone desktop application. SQL interoperability is highly recommended as it can be used in different environments.

## 2.2 EXISTING SYSTEMS

### 2.2.1 Clipperz

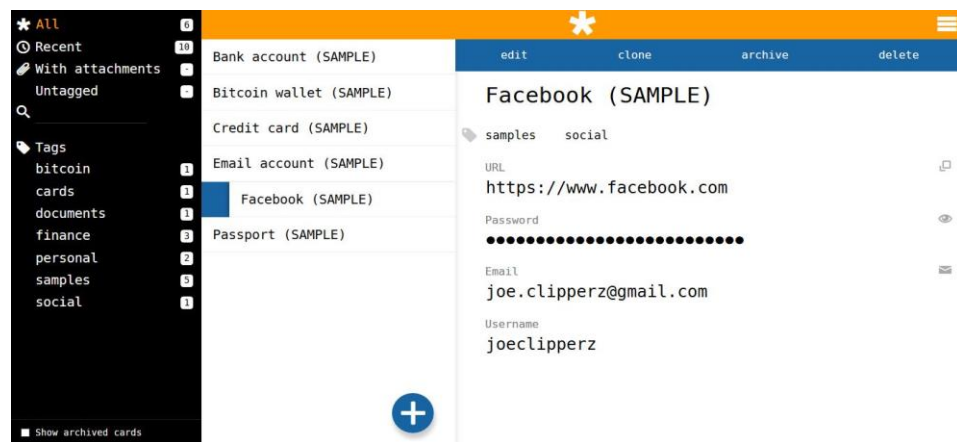


Figure 2.1 Clipperz

Clipperz is a password manager built in 2006 and founded by three programmers and researchers, Filippo Bosi, Giolio Cesare Solaroli and Marco Barulli. It is officially launched in April 2007. They are main key figures in JavaScript Crypto Library which are a repository that store cross browser cryptographic algorithms. They implement the encryption algorithm in a new project called Clipperz Password Manager. It is a free and open source. It has features of storing password, password generator, and ability to upload files and secure password sharing.

Table 2.1 Advantages and Disadvantages of Clipperz

Advantages	Disadvantages
Open source	No password rater
Free	No two-factor authentication
Password generator	Website theme color is irritating
Can upload images, audio, documents files	No secure notes
Share password	Have quota only until 100MB
Has mobile app	1 Accounts for one person only
-	No password rater

## 2.2.1 Passpack

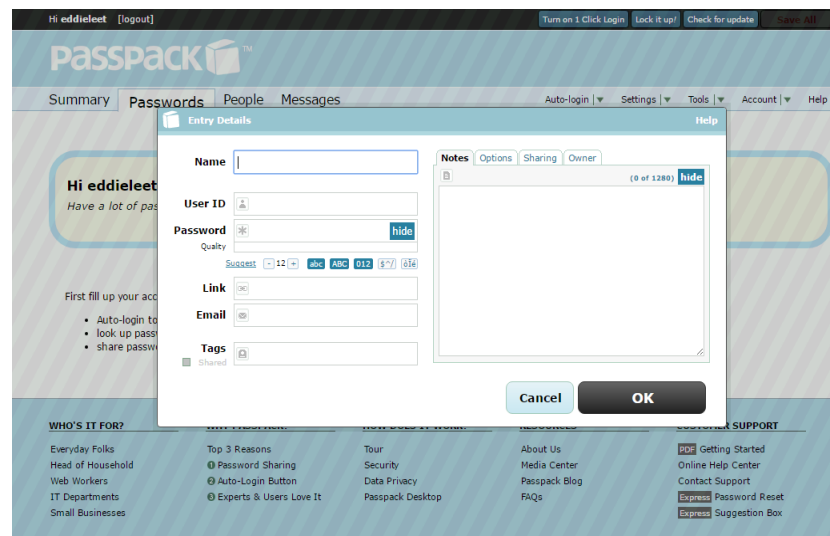


Figure 2.2 Passpack

Passpack is founded in 2006 by unknown co-founders. Their goal is helping internet users to make a password manager a free for all. The website is then acquired by Kemesa Holdings, a company that develops services for identity theft protection. Passpack main features are providing two-factor authentications, password suggestion, password sharing, import and backup services and option to send and receive messages from the different user.

Table 2.2 Advantages and Disadvantages of Passpack

Advantages	Disadvantages
Have two-factor authentications	No password rater
Has password generator	Cannot upload files
Share password	Not responsive web design in desktop websites
Import export /Backup Restore	No password rater
Has mobile sites	Cannot upload files
No mobile app	Limited features 100 Password 1 Shared User 0 Groups 1280 Notes Premium is \$1.50
Can send messages	Fonts are smalls



### 2.2.3 MyPadLock



Figure 2.3 MyPadLock Password Manager

MyPadLock Password Manager is a computer program which is password manager system made by MyPadLockTeam. It was created by using VB.NET programming language. It has minimal features of storing password, update, and delete password. It implements AES encryption. The main disadvantages are the interface is not consistent and unattractive, it only can be used by personal computer that has Windows operating systems and not portable or used in anyplace and anytime.

Table 2.3 Advantages and Disadvantages of MyPadLock

Advantages	Disadvantages
Storing passwords	Unfriendly interface and inconsistent design
Has password generator	Only works in Windows
AES Encryption	Not portable as it stored in only installed device
Import and export data	No secure notes
Store locally in hard drive	Cannot store files such as images, documents

## 2.2.4 COMPARISON OF EXISTING SYSTEMS

Table 2.4 Comparison of Three Existing Systems

<b>Name</b>	<b>Clipperz</b>	<b>PassPack</b>	<b>MyPadLock</b>
Interface of Website Design	✓	X	X
Two Factor Authentication	✓	✓	X
Save Password in Website	✓	✓	✓
Save Password in Mobile	✓	X	X
Save URLs	✓	✓	X
Save Images, Documents	✓	✓	X
Password Generator	✓	✓	X
Password Rater/Evaluator	X	✓	X
Quota for Storing Password	100MB	100 Password only for free version Pro version	Not stated
Multiple accounts in one login	X	X	X

## **CHAPTER 3**

### **INTRODUCTION**

#### **3.1 INTRODUCTION**

In this project, the software development methodologies used are Rapid Application Development which is also known as RAD. This methodology is chosen because the process of software development can be focused more than prioritizing on planning. General user interface can be developing while developing the coding process together.

## 3.2 METHODOLOGY

### 3.2.1 Justification of Chosen Methodology

The Rapid Application Development (RAD) can group into four different phases.

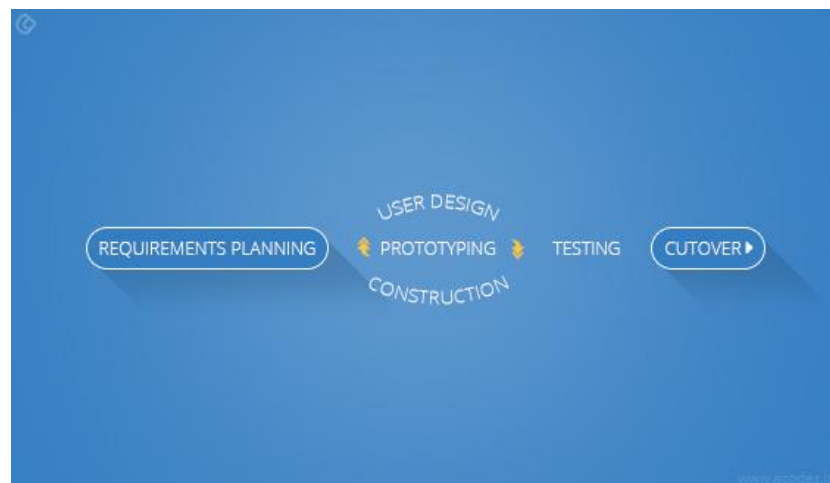


Figure 3.1 RAD phases

i. Requirement planning phase

During requirement and planning phase, discussion with supervisor is made. An appropriate title of project is selected. Chapter 1 is discussed and submitted. Chapter 1 focuses on problems statement, objectives, scopes and thesis organization. Second meeting focuses on important task in Chapter 2. Chapter 2 focuses on comparing existing systems as reference. Chapter 2 is submitted.

ii. User design phase

Third meeting with supervisor discusses important methodologies, diagrams that shows flow of system, hardware and software tools used in develop the system, Gantt chart shows the flow from beginning from the project until submission of report and approval presentation form and supervisor and examiner marking.

iii. Construction phase

The required documentation which are Software Requirements Specifications and Software Design Documents is constructed along with required diagrams which are Data Flow diagrams, Entity Relationship Diagram, Data Dictionary, User Interface as guideline and flow of systems. Code implementation is started along with testing.

iv. Cutover phase

The final phase will be focuses on finishing building prototype and testing. User training and acceptance test is done.

Report of thesis and TurnItIn report with presentation approval form is submitted before presentation in front of examiner and supervisor for marking.

The main advantages of these methodologies are;

- i. Requirement changes can be easily evaluated and done
- ii. Iteration development can be shorten
- iii. Productivity can be increase because only one developer
- iv. Development time can be reduce
- v. Can reuse many components
- vi. User feedback is highly encourage

### 3.2.2 Context Diagram

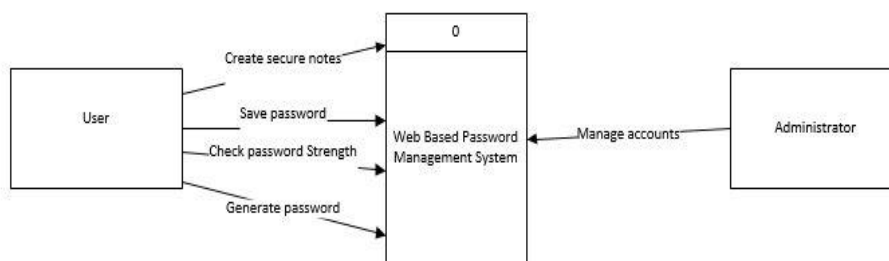


Figure 3.2 Context Diagram of System

Diagram shows the inputs and outputs of user and administrator can be done with the web based password management system. These shows the general views of function of user can used to interact with systems.

### 3.2.3 Software Requirement Specification

(Refer Appendix B)

### 3.2.4 Software Design Document

(Refer Appendix C)

### 3.2.5 Use Case Diagram

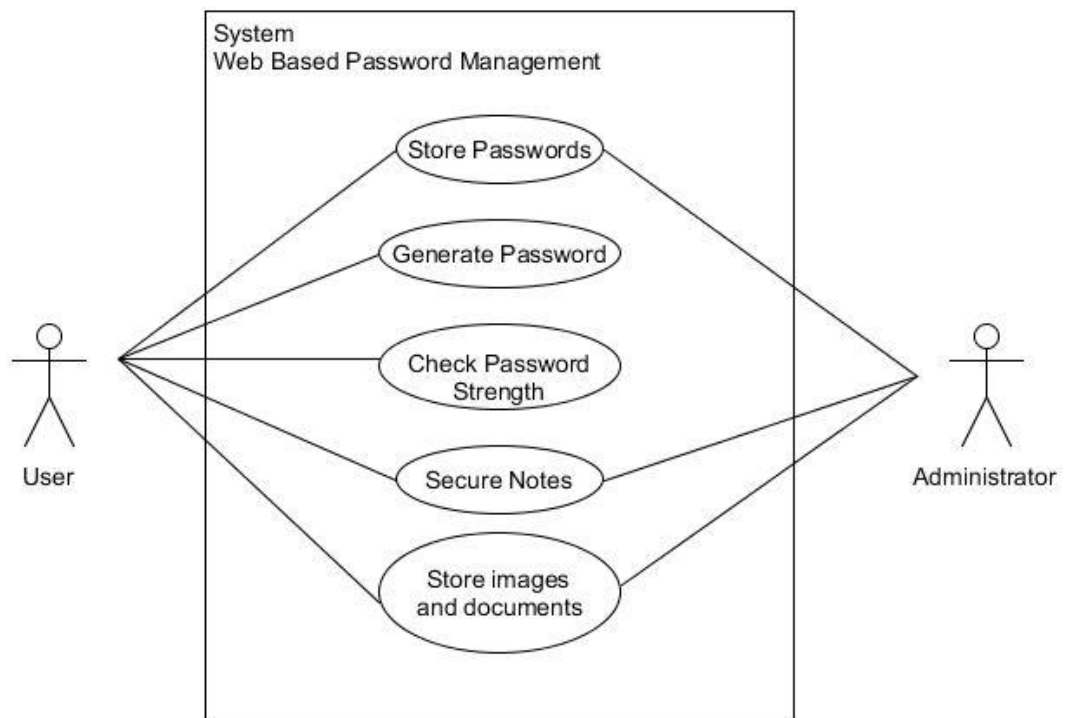


Figure 3.3 Use Case Diagram of System

The use case diagram shows the interaction of user and administrator towards the system. The user can store password, generate password, check password strength, store secure notes and documents. The information of user is encrypted using security encryption. However, administrator can know which function that is used on user but information is unknown by administrator.

### 3.2.6 Module of System

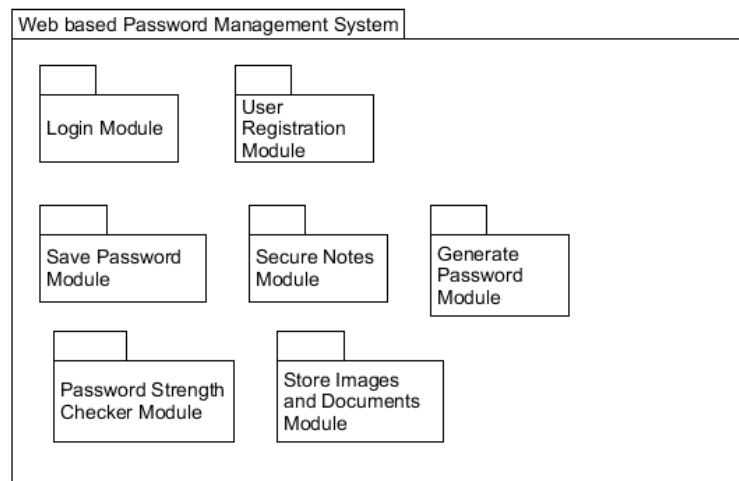


Figure 3.4 Package Diagrams of Systems

- i. **Login Module**  
User enter login information which are username and password before access their account.
- ii. **User Registration Module**  
User registers before access their account. The system will prompt user to enter name, email, username and password as login information for creating an account. The system also ask user to create their own Master Password as secondary password for better authentication and security.
- iii. **Save Password Module**  
User can save password and required information whether it is online services such as email, social media accounts, or hardware devices password such as WIFI password and phone lock pin number. User can create password, view, update and delete if necessary.
- iv. **Secure Notes Module**  
User can create notes which are secured that can store different information from password.



v. Generate Password Module

User can generate unique password according to their password and characters long.

vi. Password Strength Checker Module

User can check and evaluate their password strength and security using the tools. The tool will verify user that their strength according to level of type of combinations of characters, number and special characters.

vii. Store Images and Documents Module

User also can store private images and documents. User can upload required files, view them, updates and delete if necessary.

### 3.2.7 Dialogue Diagram

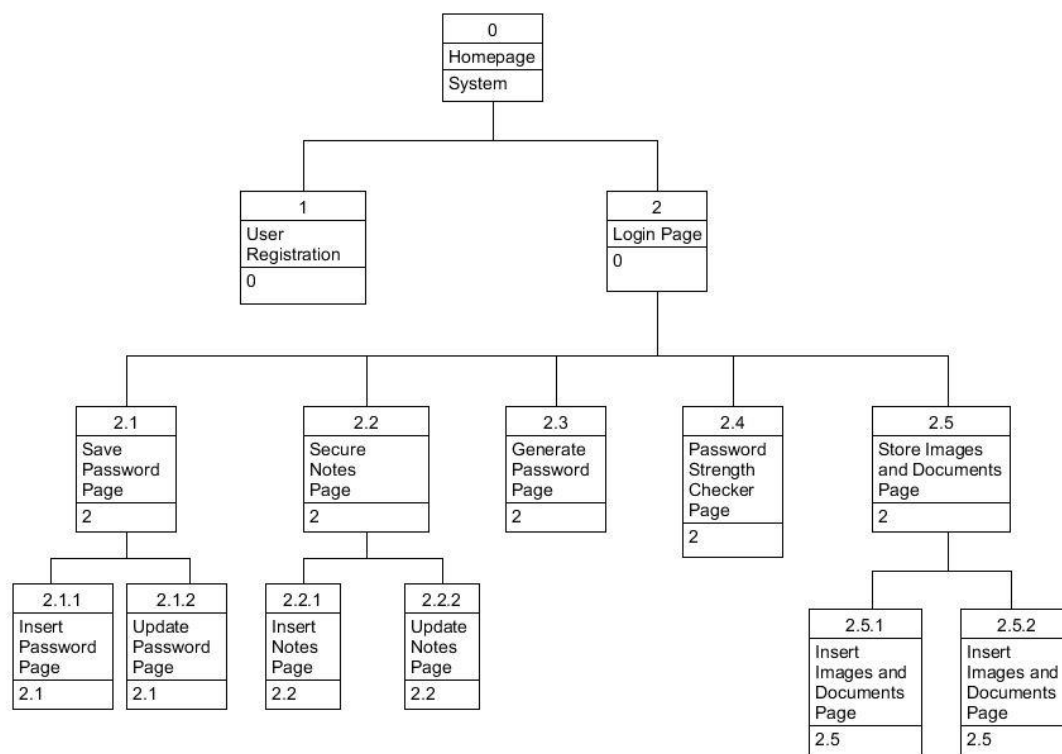


Figure 3.5 Dialogue Diagram of system.

This dialogue diagrams shows the detail and systems overview based on code implementation. User is prompt with homepage of system as introduction. The user must register email and password as their have to make an account first. The, the can continue use the system by entering the required information to the Login Page. After login, user can be use their account and capable of user five functions. Both save password, secure notes and store images and documents are capable of user to create, view, update and delete certain information that is necessary. Other functions which are generating safe and unique password and password strength checker can by user for safety password measures.

### 3.3 HARDWARE AND SOFTWARE

In this section, the hardware and software tools are used to creating diagram, setup software for server, web browser for compiling PHP codes and word processing software for creating documentations and charts.

#### 3.3.1 Hardware

Table 3.1 Hardware Tools used in development

Hardware Name	Function
HP Pavilion 15	Main computer for develop project. All software and documentation done.
Philips 160E	Secondary display for productivity during code completion.

#### 3.3.2 Software

Table 3.2 Software Tools used in development

Software Name	Version	Function
Windows 10	64 bit Home version	Main operating system for computers for development.
Google Chrome	57.0.2987.133	Main web browser for compiling web pages.
Xampp	3.3.2	A local web server installed to store web pages.
Microsoft Office Word	2010	Software for creating documentations.
Umlet	14.2	Drawing use case, dialogue diagrams
Microsoft Project	2010	Create Gantt Chart
Microsoft Visio	2013	Drawing context diagrams
Google Drive	2.34.5075.1619	Main cloud storage for backup purposes for storing images, documents, source codes of the project.

### **3.4 GANTT CHART**

(Refer Appendix A)

### 3.5 IMPLEMENTATION

The implementation of project started with collecting requirements based on comparison of existing systems. Here, we can analyses and find advantages and disadvantages of current existing system. We can produce a feature from the current ones which lack of features and have disadvantages while improving by adding and enhancing current features.

The projects started with drawing diagrams which are Use Case diagram, Context Diagram, Package Diagram and Dialogue Diagram. In this case, we can know the flow and interaction of systems by analysing the structure of diagrams. We can know certain methods, hardware, software requires, modules, functions, input and outputs that can be produced for the build prototype.

The first setup done is by installing local web server which is Xampp Apache. We can start develop the source code using a text editor name Notepad++. At the same time, we develop of the interface of website according to the flow of the diagrams.

Then, we stored the source code inside .html,.css and .php file extensions inside htdocs folders in Xampp folder in Local Hard Disk C drive directory. On top of that, we open Xampp control panel and turn on both Apache and MySQL server until both processing running and green indicator light on.. Then, we executing our internet browser which and enters localhost to check the location of folder of source code and creating database and table inside phpmyadmin by entering localhost/phpmyadmin in the URL section of the web browser.

Next, we can start testing the system by entering input to the systems and receive outputs by testing the function while executing the systems inside the local server. We can see any errors inside the web browser as it will state the source of the problems and errors.

After basic operating such as create, view, update and delete, we add encryption and decryption techniques to the code to secure our passwords. The encryption and decryption techniques that will be use either RC4 encryption or AES 256 bit encryption. However, AES 256 encryption is recommended solution for securing the information stored for the user. The encryption method was created by Vincent Rijmen and Joan Daemen. The algorithm was previously known as Rjindael cipher by both cryptographers. The United States of America government uses these encryption techniques to secure their classified information which is approved by National Security Agency. AES encryption stands for acronym of “Advanced Encryption Standard”. It has 128 bits of blocks and consists of three block of ciphers or key lengths of 128,192,256 bits. It consist of combination both secret key which must be known to the user and sender with plain text. Both information will go process of encryption with cipher and it will produced ciphered text which is random and unique. It substitutes information to the substitution table, shifting the rows of the data and mixed the columns of data and XOR operation so it can produce ciphered text.

Lastly, we can go on user training and generate user guide documentation.

### **3.6 TESTING**

In this case, we have two types of testing techniques which are used in this development of project. We include both Black Box Testing and White Box Testing techniques for evaluating the performance, security and integration of system.

In Black Box testing, we focus on testing the internal structure, design and structure which are not known by tester. This testing activity including review of documentations whether it is tally to the requirements and development of the prototype. We can do both testing levels which are User Acceptance Testing and System Testing for full assessment of the performance of system.

In White Box testing, we focus on testing activity which the internal structure, design and structure which are known by tester. We used the diagrams which are Use Case diagram, Context diagram, Package diagram and Dialogue diagrams as reference for the structure of development, interaction and modules with functions for implementation. This testing including unit testing by testing input and outputs and function of each module. Second, we evaluate and do integration testing to assess the integration of module connecting together as a whole system.

## REFERENCES

- Srl, C. (2006). Clipperz. Retrieved April 30, 2017, from <https://clipperz.is/>
- Systems development life cycle. (2017, April 20). Retrieved April 30, 2017, from [https://en.wikipedia.org/wiki/Systems\\_development\\_life\\_cycle](https://en.wikipedia.org/wiki/Systems_development_life_cycle)
- Rapid application development. (2017, April 17). Retrieved April 30, 2017, from [https://en.wikipedia.org/wiki/Rapid\\_application\\_development](https://en.wikipedia.org/wiki/Rapid_application_development)
- Passpack - Password Manager. (2015, October 08). Retrieved April 30, 2017, from <https://www.passpack.com/>
- How MyPadlock works. (2009). Retrieved April 30, 2017, from <http://mypadlock.com/Home/HowItWorks>
- T. (n.d.). Advanced Encryption Standard. Retrieved May 02, 2017, from [https://www.tutorialspoint.com/cryptography/advanced\\_encryption\\_standard.htm](https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm)



ID	Task Mode	Task Name	Duration	Start	Finish	12 Feb '17				5 Mar '17				26 Mar '17
						S	S	M	T	W	T	F		
1		Requirement & Planning Phase												
2		First meeting with Supervisor	4 days	Mon 13/2/17	Thu 16/2/17									
3		Submit Title Form	1 day	Fri 17/2/17	Fri 17/2/17									
4		Discussion on Chapter 1	10 days	Sat 18/2/17	Thu 2/3/17									
5		Submission on Chapter 1	1 day	Fri 3/3/17	Fri 3/3/17									
6		Second Meeting	1 day	Fri 3/3/17	Fri 3/3/17									
7		Discussion on Chapter 2	10 days	Sat 4/3/17	Thu 16/3/17									
8		Submission on Chapter 2	1 day	Fri 17/3/17	Fri 17/3/17									
9		Submission of Progress Form	1 day	Fri 17/3/17	Fri 17/3/17									
10		User Design Phase												
11		Third Meeting	1 day	Fri 17/3/17	Fri 17/3/17									
12		Discussion on Chapter 3	16 days	Sat 18/3/17	Fri 7/4/17									
13		Structure Diagrams	5 days	Sat 8/4/17	Thu 13/4/17									
14		Submission on Chapter 3	1 day	Fri 14/4/17	Fri 14/4/17									
15		Construction Phase												
16		Structure SRS Documents	5 days	Sat 15/4/17	Thu 20/4/17									
17		Structure SDD Documents	4 days	Mon 24/4/17	Thu 27/4/17									
18		Start Code Implementation	12 days	Sat 15/4/17	Sun 30/4/17									
19		Testing	11 days	Mon 17/4/17	Sun 30/4/17									
20		Cutover Phase												
21		Finish Testing and Build Prototype	11 days	Mon 17/4/17	Sun 30/4/17									
22		User Training	3 days	Mon 1/5/17	Wed 3/5/17									

Project: Gantt Chart PSM1  
Date: Fri 14/4/17

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

ID	Task Mode	Task Name	Duration	Start	Finish	12 Feb '17				5 Mar '17				26 Mar '17
						S	S	M	T	W	T	F		
23		Submit Report	1 day	Thu 4/5/17	Thu 4/5/17									
24		Submit Turnitin Report	1 day	Thu 4/5/17	Thu 4/5/17									
25		Submit Presentation Approval Form	1 day	Thu 4/5/17	Thu 4/5/17									
26		Examiner Marking	2 days	Sun 14/5/17	Mon 15/5/17									
27		Supervisor Marking	36 days	Wed 17/5/17	Wed 5/7/17									

Project: Gantt Chart PSM1 Date: Fri 14/4/17	Task		External Milestone		Manual Summary Rollup	
	Split		Inactive Task		Manual Summary	
	Milestone		Inactive Milestone		Start-only	
	Summary		Inactive Summary		Finish-only	
	Project Summary		Manual Task		Deadline	
	External Tasks		Duration-only		Progress	

2017

# SOFTWARE REQUIREMENT SPECIFICATION (SRS)

WEB BASED PASSWORD  
MANAGEMENT SYSTEM

---

Faculty Computer System & Software  
Engineering (FSKKP)

Chavalit A/L Tat Wi  
CB141414



## TABLE OF CONTENT

<b>1.0</b>	<b>FUNCTIONS.....</b>	<b>1</b>
<b>2.0</b>	<b>DATA FLOWDIAGRAM LEVEL0 (DFD LEVEL 0).....</b>	<b>2</b>
<b>3.0</b>	<b>DATA FLOW LEVEL 1 (DFD LEVEL 1).....</b>	<b>3</b>
<b>4.0</b>	<b>ALGORITHM OR STRUCTURED ENGLISH.....</b>	<b>6</b>
	4.1 User Registration.....	6
	4.2 Login .....	6
	4.3 Save Password.....	7
	4.4 Secure Notes.....	7
	4.5 Generate Password.....	8
	4.6 Password Strength Checker.....	8
	4.7 Upload Files.....	9
<b>5.0</b>	<b>DATA MODELLING (ERD).....</b>	<b>10</b>
<b>6.0</b>	<b>SYSTEM REQUIREMENTS APPROVAL.....</b>	<b>11</b>

## **LIST OF FIGURES**

FIGURE 2.1 DFD LEVEL-0.....	2
FIGURE 3.1 USER REGISTRATION.....	3
FIGURE 3.2 LOGIN.....	3
FIGURE 3.3 SAVES PASSWORDS.....	4
FIGURE 3.4 SECURE NOTES.....	4
FIGURE 3.5 GENERATE PASSWORD.....	4
FIGURE 3.6 PASSWORD STRENGTH CHECKER .....	5
FIGURE 3.7 STORE IMAGES AND DOCUMENTS.....	5
FIGURE 5.1 DATA MODELLING (ERD) OF SYSTEM.....	10

## LIST OF TABLES

TABLE 1.1 FUNCTIONS AND DESCRIPTIONS.....	1
TABLE 4.1 USER REGISTRATION.....	6
TABLE 4.2 LOGIN.....	6
TABLE 4.3 SAVES PASSWORDS.....	7
TABLE 4.4 SECURE NOTES.....	7
TABLE 4.5 GENERATE PASSWORD.....	8
TABLE 4.6 PASSWORD STRENGTH CHECKER.....	8
TABLE 4.7 STORE IMAGES AND DOCUMENTS.....	9

## 1.0 Functions

Table 1.1 Functions and Description

Functions	Description
Login	User enter login information which are username and password before access their account.
User Registration	User registers before access their account. The system will prompt user to enter name, email, username and password as login information for creating an account. The system also ask user to create their own Master Password as secondary password for better authentication and security.
Store Password	User can save password and required information whether it is online services such as email, social media accounts, or hardware devices password such as WIFI password and phone lock pin number. User can create password, view, update and delete if necessary.
Secure Notes	User can create notes which are secured that can store different information from password.
Generate Password	User can generate unique password according to their password and characters long.
Password Strength Checker	User can check and evaluate their password strength and security using the tools. The tool will verify user that their strength according to level of type of combinations of characters, number and special characters.
Store Images and Documents	User also can store private images and documents. User can upload required files, view them, updates and delete if necessary.

## 2.0 DATA FLOW DIGRAM LEVEL 0 (DFD LEVEL-0)

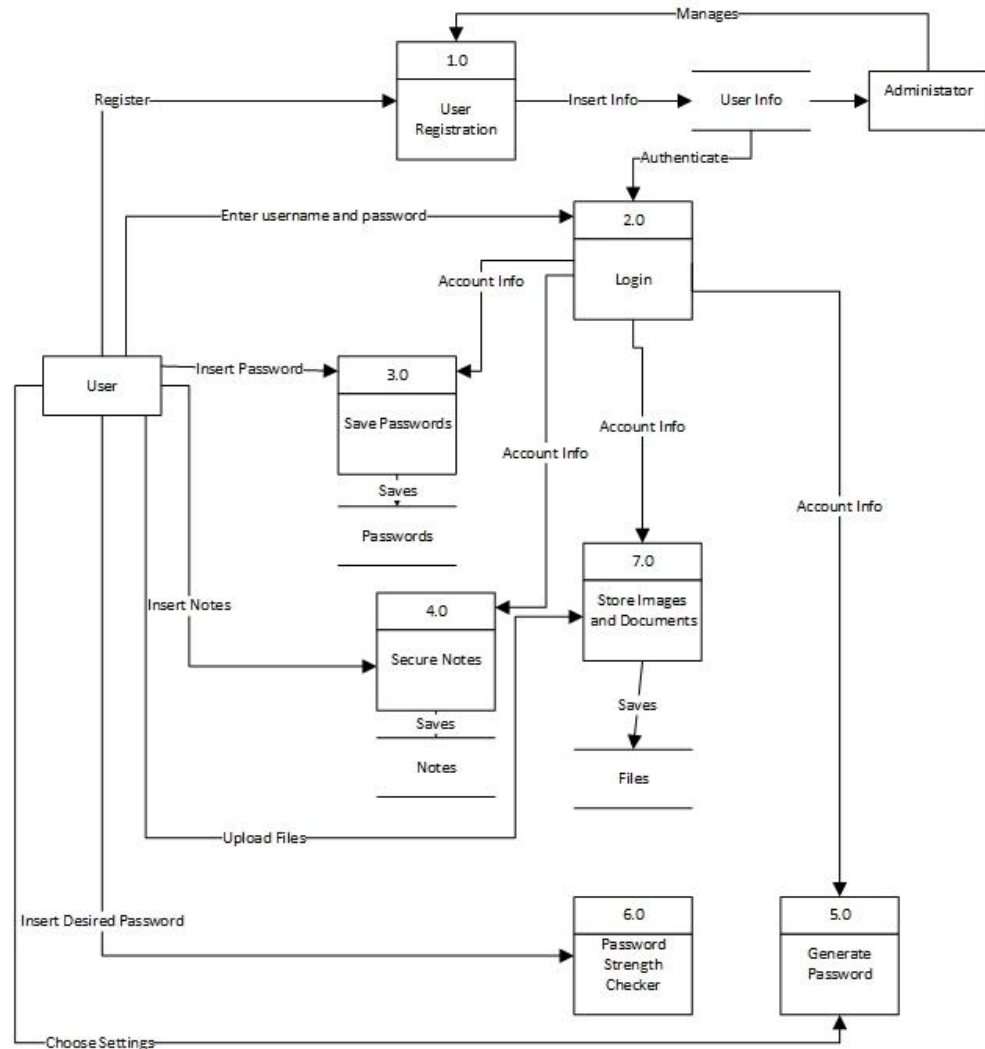


Figure 2.1 DFD Level-0

Figure 2.1 describes the data flow diagram level 0 for the Password Management System. It consists of two entities which are Administrator and User. Administrator manages user registration which is their accounts information. User has many functions which they can use. User can save passwords, secure notes and upload images and documents which are stored in database. User can also check their password strength and generate unique password.



### 3.0 DATA FLOW DIGRAM LEVEL 1 (DFD LEVEL- 1)

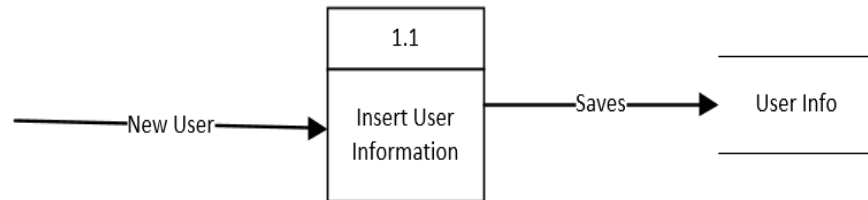


Figure 3.1 User Registration

Figure 3.1 describes the new user will register first for making accounts and will fill required information which are email, username, password and age.

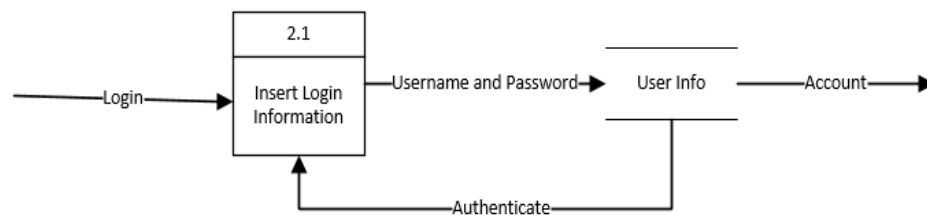


Figure 3.2 Login

Figure 3.2 describe that user that already make an account can enter their username and password. The information is then check in database for authentication to make sure that user enter the correct information for login.

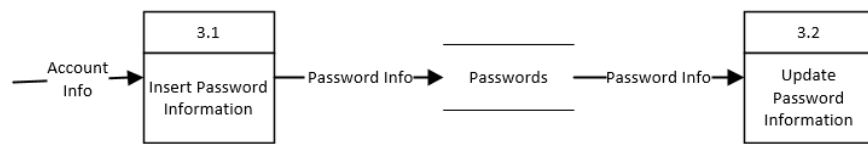


Figure 3.3 Save Passwords

Figure 3.3 describe the user that already login can use the functions inside the system. User can enter required information such as the name of website, the URL of the website, the username and password of the website or any related information.

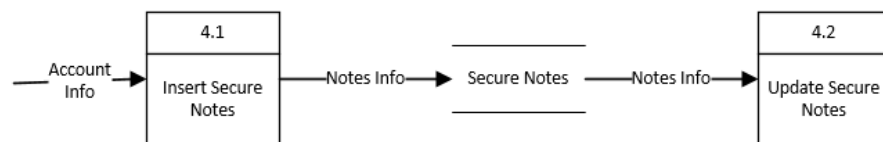


Figure 3.4 Secure Notes

Figure 3.4 describes the user can store notes inside secure notes.



Figure 3.5 Generate Password

Figure 3.5 describes user can generate unique password. The user can choose the settings which can let them choose the length of character. Then, user click Generate, a unique secure password is displayed.

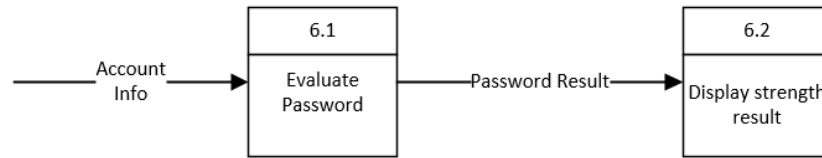


Figure 3.6 Password Strength Checker

Figure 3.6 describes the user can evaluate the password strength using the function inside the system. They have to enter the password, and it will display result the strength of password.

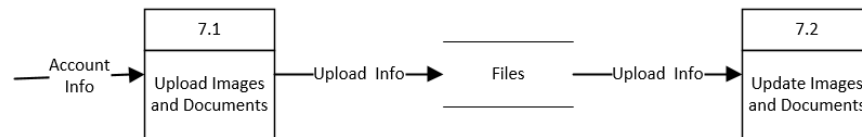


Figure 3.7 Store Images and Documents

Figure 3.7 describes the user can store images and documents to the system. The user can upload images and documents with appropriate files types that recognizable it will display it. The user can edit and delete any files they want.

## 4.0 STRUCTURED ENGLISH

### 4.1 User Registration

Table 4.1 User Registration

Responsibility	To registers an account by entering name, email, username and password as login information for creating an account.
Algorithm	BEGIN INSERT name INSERT email INSERT username INSERT password INSERT confirmation password INSERT master password END

### 4.2 Login

Table 4.2 Login

Responsibility	To enter login information which username and password before access their accounts.
Algorithm	BEGIN INSERT username INSERT password INSERT master password END

### 4.3 Save Passwords

Table 4.3 Save Passwords

Responsibility	To save password and required information whether it is online services such as email, social media accounts, or hardware devices password such as WIFI password and phone lock pin number. User can create password, view, update and delete if necessary.
Algorithm	BEGIN INSERT id INSERT title INSERT password INSERT URL INSERT description END

### 4.4 Secure Notes

Table 4.4 Secure Notes

Responsibility	To create notes which are secured that can store different information from password.
Algorithm	BEGIN INSERT id INSERT title INSERT notes END

#### 4.5 Generate Password

Table 4.5 Generate Password

Responsibility	To generate unique password according to their password and characters long.
Algorithm	BEGIN INSERT configuration OUTPUT unique password END

#### 4.6 Password Strength Checker

Table 4.6 Password Strength Checker

Responsibility	To check and evaluate their password strength and security using the tools.
Algorithm	BEGIN INSERT check password OUTPUT checked password END

## 4.7 Store Images and Documents

Table 4.7 Store Images and Documents

Responsibility	To can store images and documents.
Algorithm	<pre>BEGIN INSERT id INSERT title INSERT file description INSERT files END</pre>

## 5.0 DATA MODELLING (ERD)

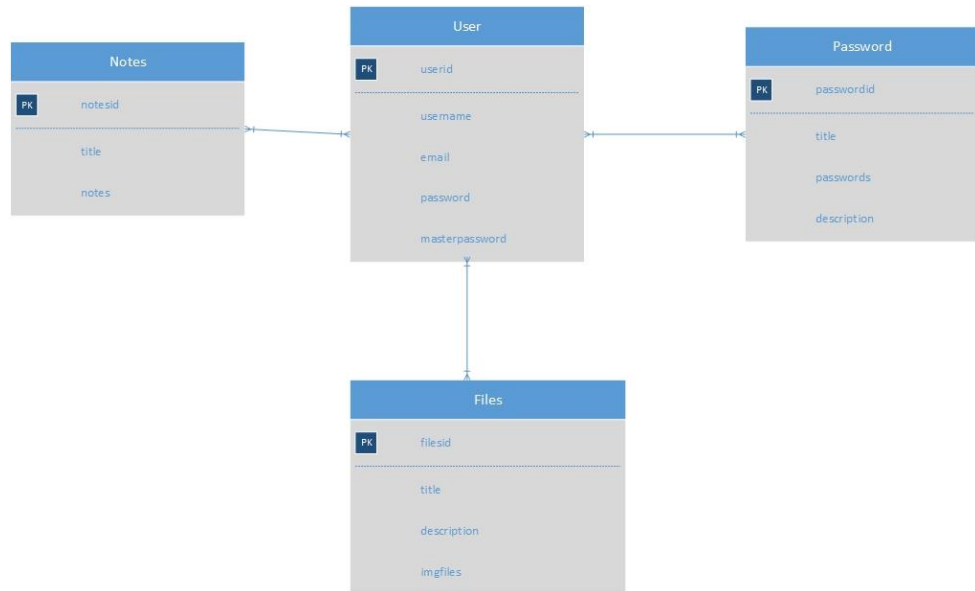


Figure 5.1 Data Modelling (ERD) of system



## 6.0 SYSTEM REQUIREMENTS APPROVAL

	Name	Date
<b>Verified by:</b>  <hr/>		
Developer		
<b>Verified by:</b>  <hr/>		
Client		

2017

# SOFTWARE DESIGN DOCUMENT (SDD)

WEB BASED PASSWORD  
MANAGEMENT SYSTEM

---

Faculty Computer System & Software  
Engineering (FSKKP)

Chavalit A/L Tat Wi  
CB14144



## TABLE OF CONTENT

<b>1.0 DATA DICTIONARY.....</b>	<b>1</b>
1.1 User Entity .....	1
1.2 Notes Entity .....	1
1.3 Password Entity .....	2
1.4 Files Entity .....	2
<b>2.0 USER INTERFACE.....</b>	<b>3</b>
2.1 User Registration Page .....	3
2.2 Login Page .....	4
2.3 Save Password Page .....	5
2.4 View Password Page .....	6
2.5 Update Password Page .....	7
2.6 Generate Password Page .....	8
2.7 Secure Notes Page .....	9
2.8 View Secure Notes Page.....	10
2.9 Update Secure Notes Page .....	11
2.10 Password Strength Checker Page .....	12
2.11 Upload Files Page .....	13
2.12 View Uploaded Files Page .....	14
2.13 View Passwords (Administrator) Page .....	15
2.14 View Secure Notes (Administrator) Page .....	16
<b>3.0 SYSTEM DESIGN APPROVAL.....</b>	<b>17</b>

## LIST OF FIGURES

FIGURE 2.1 USER REGISTRATION PAGE.....	3
FIGURE 2.2 LOGIN INTERFACE PAGE.....	4
FIGURE 2.3 SAVES PASSWORDS PAGE .....	5
FIGURE 2.4 VIEWS PASSWORDS PAGE .....	6
FIGURE 2.5 UPDATE PASSWORDS PAGE .....	7
FIGURE 2.6 GENERATE PASSWORD PAGE .....	8
FIGURE 2.7 SECURE NOTES PAGE .....	9
FIGURE 2.8 VIEW SECURE NOTES PAGE.....	10
FIGURE 2.9 UPDATE SECURE NOTES PAGE .....	11
FIGURE 2.10 PASSWORD STRENGTH CHECKER PAGE .....	12
FIGURE 2.11 UPLOAD FILES PAGE .....	13
FIGURE 2.12 VIEW UPLOADED FILES PAGE .....	14
FIGURE 2.13 VIEW PASSWORDS (ADMINISITRATOR) PAGE ...	15
FIGURE 2.14 VIEW SECURE NOTES (ADMINISITRATOR) PAGE	16

**LIST OF TABLES**

TABLE 1.1 USER ENTITY..... 1

TABLE 1.1 NOTES ENTITY..... 1

TABLE 1.2 PASSWORD ENTITY..... 2

TABLE 1.3 FILES ENTITY..... 2

## 1.0 DATA DICTIONARY

### 1.1 User Entity

Table 1.1: User entity

Field Name	Description	Data Type	Constraint
user_id	Define user's id	VARCHAR(10)	PRIMARY KEY
user_name	Define username	VARCHAR(50)	
user_email	Define email	VARCHAR(30)	
user_password	Define password	VARCHAR(30)	
user_masterpassword	Define master password	VARCHAR(30)	

### 1.2 Notes Entity

Table 1.2: Notes entity

Field Name	Description	Data Type	Constraint
notes_id	Define notes' id	VARCHAR(10)	PRIMARY KEY
notes_title	Define titles of notes	VARCHAR(30)	
notes_desc	Define description of notes	VARCHAR(150)	

### 1.3 Password Entity

Table `1.3: Password entity

Field Name	Description	Data Type	Constraint
password_id	Define password's id	VARCHAR(10)	PRIMARY KEY
password_name	Define title of password	VARCHAR(30)	
password_save	Define password that wanted to be save	VARCHAR(30)	
password_desc	Define the description of password	VARCHAR(150)	

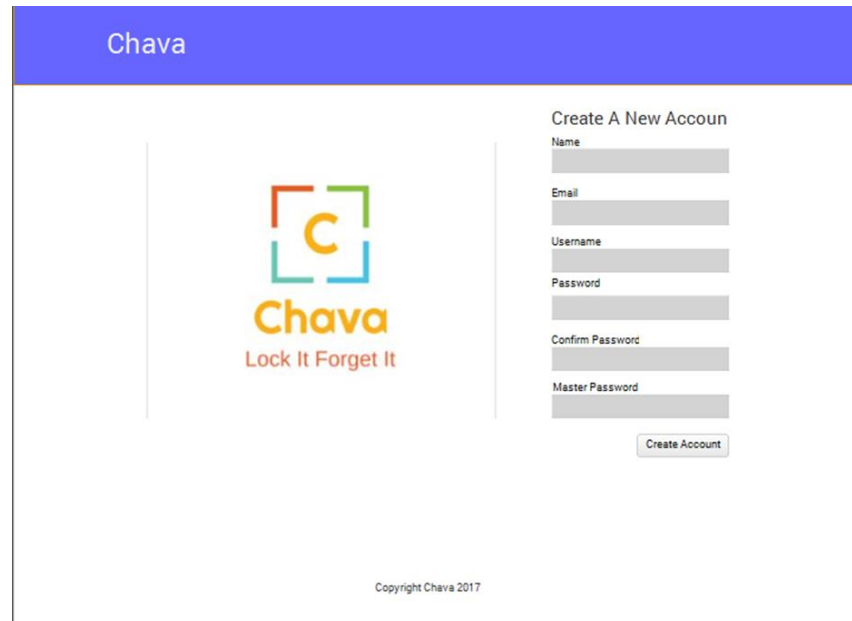
### 1.4 Files Entity

Table 1.4: Files entity

Field Name	Description	Data Type	Constraint
files_id	Define files' id	VARCHAR(10)	PRIMARY KEY
files_name	Define name of file	VARCHAR(30)	
files_desc	Define description of file	VARCHAR(150)	
files_imgfiles	Define the file uploaded	VARCHAR(200)	

## 2.0 USER INTERFACE

### 2.1 User Registration Page



The screenshot displays the 'Chava' user registration interface. At the top, a blue header bar contains the word 'Chava'. The main content area is divided into two sections by a vertical line. On the left, the 'Chava' logo is centered, featuring a stylized 'C' in a square frame with the text 'Chava' and 'Lock It Forget It' below it. On the right, under the heading 'Create A New Account', there are six input fields: 'Name', 'Email', 'Username', 'Password', 'Confirm Password', and 'Master Password'. A 'Create Account' button is positioned below these fields. At the bottom center, a small copyright notice reads 'Copyright Chava 2017'.

Figure 2.1: User Registration Page

Figure 2.1 shows that potential user have to enter information to create an account so that can use the system. They have to enter name, email, username, password, another password that validates both password inserted before is same, and a master password which they can use as security password. After they make an account, they will be redirected to Login Page so that they can try use their username, password and master password as a confirmation for making an account.



## 2.2 Login Page



The screenshot displays the Chava login interface. At the top, a blue header bar contains the 'Chava' logo. The main content area is divided into two sections by a vertical line. On the left, there is a large, stylized 'C' logo composed of four colored squares (red, green, blue, and yellow) surrounding a central orange 'C'. Below this logo, the text 'Chava' is written in orange, followed by the tagline 'Lock It Forget It' in a smaller, lighter font. On the right side, the 'Login' section features three input fields labeled 'Username', 'Password', and 'Master Password'. A 'Login' button is positioned below these fields, and a link for 'Forgot Password?' is located at the bottom of the login section. At the very bottom of the page, a small copyright notice reads 'Copyright Chava 2017'.

Figure 2.2 Login Page

Figure 2.2 shows the Login page. The user that already registered and administrator can enter their username, password and master password before accessing their account. The correct entered information will redirected the user of system to the password page.

## 2.3 Save Password Page

Chava

Welcome Chavali Logout

Home Secure Notes Generate Strength Checker Storage

Save Password

Name

Username

Password

URL

Description

Clear Save

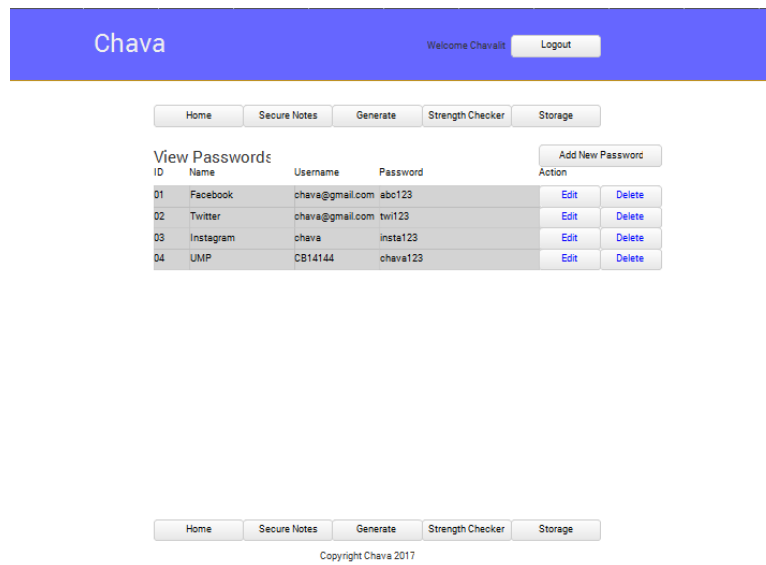
Home Secure Notes Generate Strength Checker Storage

Copyright Chava 2017

Figure 2.3 Save Password Page

Figure 2.3 shows the Password page. The user can insert the name of website or services, or hardware devices they used, username, password, URL as an option, and description if they want to add something. They have to click 'Save' button to save the information to the database. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.4 View Passwords Page



2.4 : View Passwords Page

Figure 2.4 shows the View Password page. This page shows the list of all passwords that have been saved to the database. The page will retrieve all information that has been inserted on their respective accounts. The user of the account can edit the current passwords they want or delete it. When a user wants to edit the information, they will be directed to the update password page. If the user wants to delete the password they want, they will be prompted with a confirmation popup message before confirming the delete.

## 2.5 Update Passwords Page

Chava

Welcome Chavalt Logout

Home Secure Notes Generate Strength Checker Storage

Update Password

Name  
Facebook

Username  
chava@gmail.com

Password  
chava123

URL  
www.facebook.com

Description  
Main Facebook Account

Clear Save

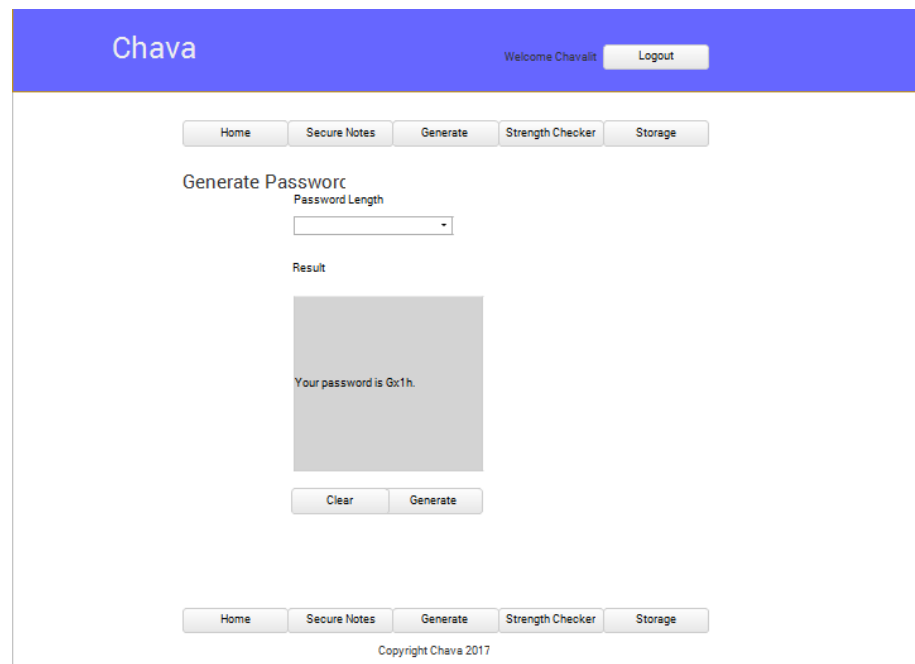
Home Secure Notes Generate Strength Checker Storage

Copyright Chava 2017

Figure 2.5: Update Password Page

Figure 2.5 shows the Update Password page. This page shows the list of all passwords that have been saved to database. The page will retrieve all information that have been inserted on their respective accounts. The user of account can edit the current passwords they wanted or delete it. When user want to edit the information they will be directed to the update password page. If the user want to delete the password they want, they will prompt will a confirmation popup message before confirm for delete. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.6 Generate Password Page



The screenshot shows a web application interface for a password generator. At the top, a blue header bar contains the text "Chava" on the left, "Welcome Chavalit" in the center, and a "Logout" button on the right. Below the header is a navigation bar with five buttons: "Home", "Secure Notes", "Generate", "Strength Checker", and "Storage". The main content area is titled "Generate Password" and contains a "Password Length" dropdown menu. Below this is a "Result" section with a large gray box displaying the text "Your password is 0x1h.". At the bottom of the result box are two buttons: "Clear" and "Generate". A second navigation bar with the same five buttons is located at the bottom of the page, above the footer text "Copyright Chava 2017".

Figure 2.6: Generate Password Page

Figure 2.6 shows the Password Generator page. The user will have to choose the desired length of password they wanted. Then, they have to click 'Generate' button to display the output based on the length they choose. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.7 Secure Notes Page

Chava

Welcome Chavalit Logout

Home Secure Notes Generate Strength Checker Storage

Secure Notes

Title

Description

Clear Save

Home Secure Notes Generate Strength Checker Storage

Copyright Chava 2017

Figure 2.7: Secure Notes Page

Figure 2.7 shows the Secure Notes page. The user can insert the title and description of notes that wanted to save. They have to click 'Save' button to save the information to the database. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.8 View Secure Notes Page



Figure 2.8: View Secure Notes Page

Figure 2.8 shows the View Secure Notes Page. This page shows the list of all notes that have been save to database. The page will retrieve all information that have been inserted on their respective accounts. The user of account can edit the current notes they wanted or delete it. When user want to edit the information they will be directed to the update password page. If the user want to delete the notes they want, they will prompt will a confirmation popup message before confirm for delete.

## 2.9 Update Secure Notes Page

Chava

Home Secure Notes Generate Strength Checker Storage

Secure Notes

Title  
Groceries List

Description  
Banana Mango Juice

Clear Save

Home Secure Notes Generate Strength Checker Storage

Copyright Chava 2017

Figure 2.9: Update Secure Notes Page

Figure 2.9 shows the Update Secure Notes page. This page shows the list of all notes that have been saved to database. The page will retrieve all information that have been inserted on their respective accounts. The user of account can edit the current notes they wanted or delete it. When user want to edit the information they will be directed to the update secure notes page. If the user want to delete the notes they want, they will prompt with a confirmation popup message before confirm for delete. If they want to clear all information inside the textbox, they just have to click 'Clear' button.



## 2.10 Password Strength Checker Page

The screenshot shows the 'Password Strength Checker' page within the 'Chava' application. The top navigation bar is blue with the 'Chava' logo on the left, 'Welcome Chavalit' in the center, and a 'Logout' button on the right. Below the navigation bar is a horizontal menu with five buttons: 'Home', 'Secure Notes', 'Generate', 'Strength Checker', and 'Storage'. The 'Strength Checker' button is currently selected. The main content area is titled 'Password Strength Checke' (note the typo). Below the title is a 'Password' label followed by a text input field containing 'chava123'. Underneath the input field is a 'Result' label followed by a large gray rectangular box. Inside this box, the text 'Your password is Weak.' is displayed. Below the result box is a 'Clear' button. At the bottom of the page, there is another horizontal menu identical to the one above, and a footer line that reads 'Copyright Chava 2017'.

Figure 2.10: Password Strength Checker Page

Figure 2.10 shows the Update Password page. This page shows an unique tool for evaulation password strength. They can do it by typing the password that they wanted or currently use. The output of the result of the srength of the password will be shown indicating they have weak, normal or strong strength. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.11 Upload Files Interface

The screenshot shows the 'Chava' application interface for uploading files. The top navigation bar is blue and contains the application name 'Chava', a user greeting 'Welcome Chavalit', and a 'Logout' button. Below this is a secondary navigation bar with buttons for 'Home', 'Secure Notes', 'Generate', 'Strength Checker', and 'Storage'. The main content area is titled 'Store Images and Document' and contains the following form elements:

- Album Name:** A text input field.
- Name:** A text input field.
- Upload:** A text input field with a 'Browse...' button next to it.
- Description:** A larger text input area.
- Buttons:** 'Clear' and 'Save' buttons at the bottom of the form.

The bottom of the page features a footer bar with the same navigation buttons as the top bar and the text 'Copyright Chava 2017'.

Figure 2.11: Upload Files Page

Figure 2.11 shows the Upload Files page. They have to insert an album name, name of file if they want to change, browse for file that to be upload, an enter some description as a caption. The current files accepted types or extension that will be accepted are JPEG,PNG,DOC and DOCX. If they want to clear all information inside the textbox, they just have to click 'Clear' button.

## 2.12 View Uploaded Files Page

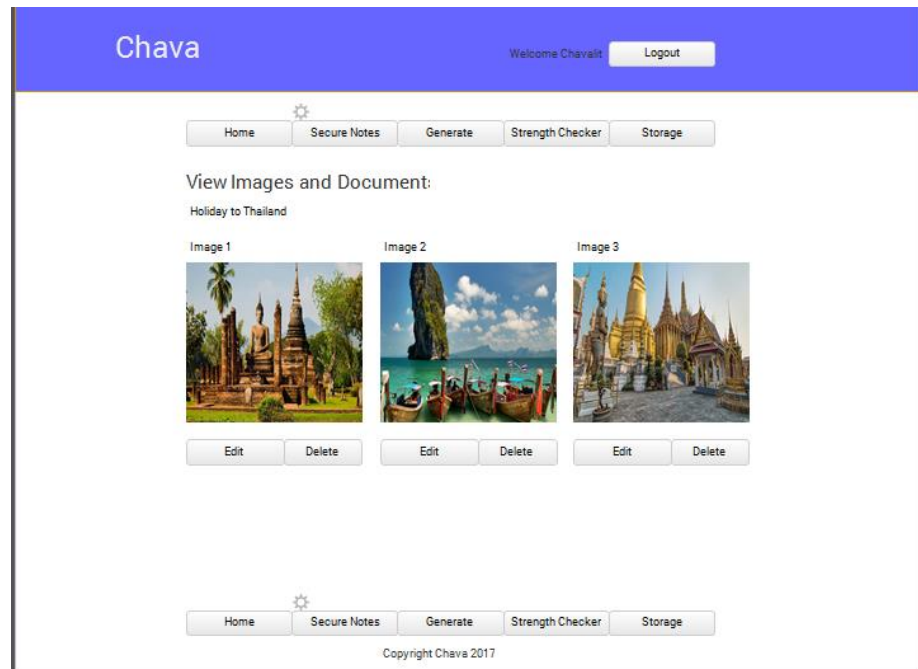


Figure 2.12 : View Uploaded Files Page

Figure 2.12 shows the View Uploaded Files Page. This page shows the list of all files that have been save to database. The page will retrieve all information that have been inserted. The user of account can edit the current images they wanted or delete it. When user want to edit the information they will be directed to the update files page. If the user want to delete the files they want, they will prompt will a confirmation popup message before confirm for delete.

## 2.13 Views Passwords (Administrator) Page

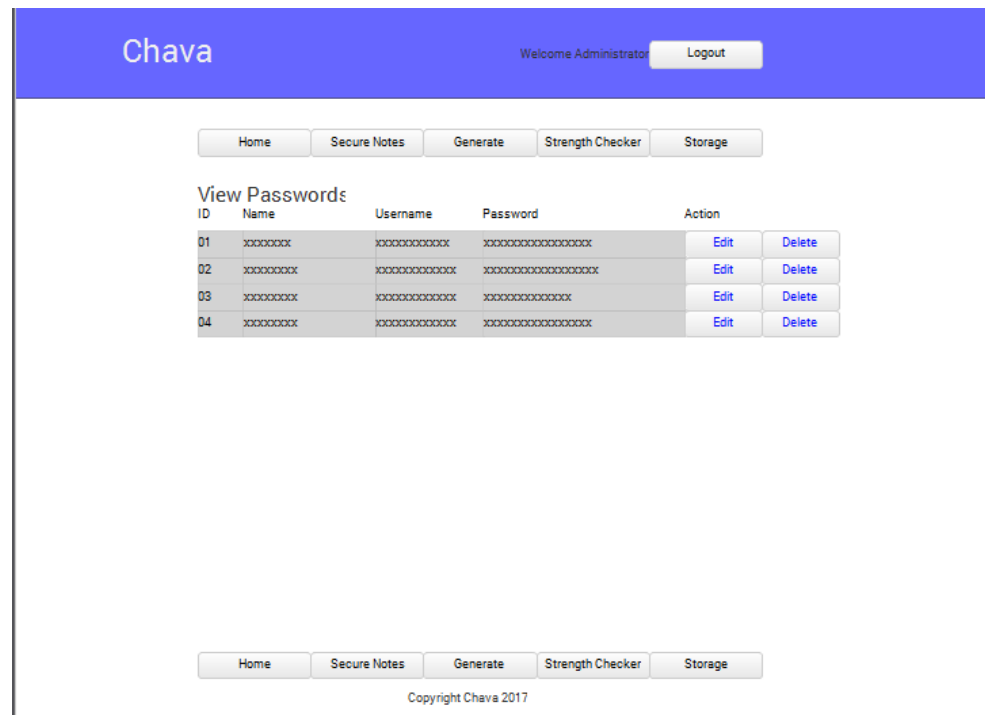


Figure 2.13: View Passwords (Administrator) Page

Figure 2.13 shows the View Password page for Administrator. This page shows the list of all passwords that have been save to database. The page will retrieve all information that have been inserted. The administrator of account can edit the current passwords they wanted or delete it. However, they cannot see information because it is encrypted. If the administrator want to delete the password they want, they will prompt will a confirmation popup message before confirm for delete.

## 2.14 Views Secure Notes (Administrator) Page

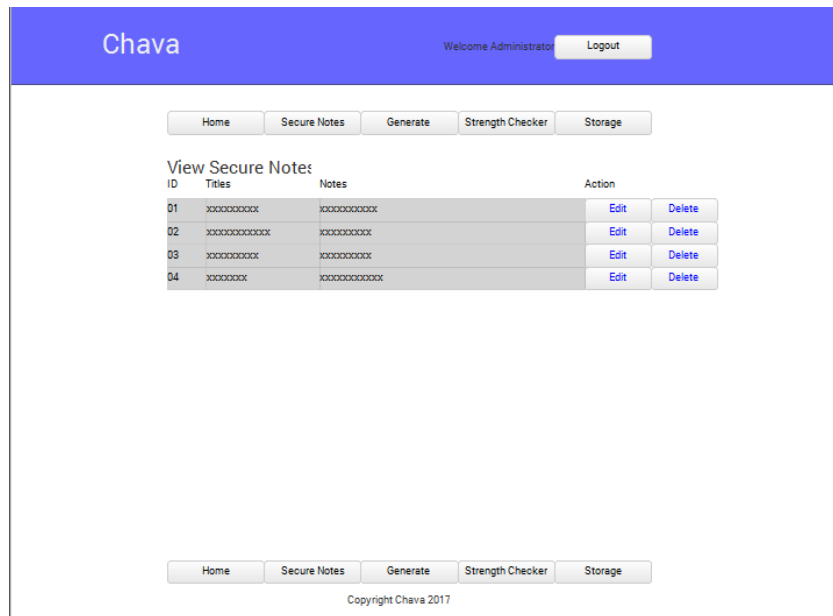


Figure 2.14: Views Secure Notes (Administrator) Page

Figure 2.14 shows the View Secure Notes page for Administrator. This page shows the list of all notes that have been save to database. The page will retrieve all information that have been inserted. The administrator of account can edit the current notes they wanted or delete it. However, they cannot see information because it is encrypted. If the administrator want to delete the notes they want, they will prompt will a confirmation popup message before confirm for delete.

### 3.0 SYSTEM DESIGN APPROVAL

	Name	Date
<b>Verified by:</b>  <hr/>		
Developer		
<b>Verified by:</b>  <hr/>		
Client		