**ABSTRACT**

**Nowadays we need to remember many passwords. One needs a password for the Windows network logon, e-mail account, online passwords, community group pages, study forums etc. The list is endless. Also, we should use different passwords for each account due to security issues.Most of the online accounts require passwords which should include letters, digits and special characters in order to increase its complexity. In order to remember their passwords belonging to multiple accounts, people tend to write down passwords on paper which makes it completely defenceless.Is there a method to remember all these passwords, or even better, store them all in a computerised private locker, in a manner such that no person other than the owner has access to the passwords? Our project provides the user an easy to use application wherein he can lock up all his passwords and retrieve them when needed.**

**Password Wallet is a password manager, which helps us to manage our passwords in a secure way. We can put all our passwords in one database, which is locked with one master key or a key file. So we only have to remember one single master password or select the key file to unlock the whole database. The database is encrypted using one of the best and most secure encryption algorithms currently known (AES 256).**

**The passwords are encrypted using SHA-256 and AES encryption techniques which keep the passwords secure and safe against intruders. Cracking a 256 bit AES key with a state-of-the-art supercomputer would take longer than the presumed age of the universe. Also, the hashing and encryption will give a 2-folded protection to the passwords and even a direct access to the database is useless as all that the intruder gets hold of is encrypted segments of code.The bottom line is that if AES could be compromised, the world would come to a standstill. The difference between cracking the AES-128 algorithm and AES-256 algorithm is considered minimal. Whatever breakthrough might crack 128-bit will probably also crack 256-bit.In the end, AES has never been cracked yet and is safe against any brute force attacks contrary to belief and arguments. However, the key size used for encryption should always be large enough that it could not be cracked by modern computers despite considering advancements in processor speeds based on Moore's law.**

**INDEX**

**Chapter No. Particulars Page No.**

**Abstract i**

**List of Figures iv**

**List of Tables v**

**1 Introduction 1**

1.1. Overview 1

1.2. Types of Passwords Managers 1

1.3. Description of password wallet 2

1.4. Implementation of AES encryption and SHA-256 2

**2 Software requirements specification 4**

2.1. Introduction 4

2.2. Overall Description 5

2.3. System Features 6

**3 Analysis 9**

3.1. Existing System 9

3.2. Drawbacks of Existing System 9

3.3. Proposed System 9

3.4. Merits of the Proposed System 9

3.5. Feasibility Study 10

3.6. Scope of the Project 11

**4 Requirements 12**

4.1. Software Requirements 12

4.1.1. Java Platform 12

4.1.2. Java Development Kit 12

4.1.3. MS Access Database 12

4.2. Hardware Requirements 13

**5 Design 14**

5.1. Unified Modeling Language Diagrams 14

5.2. Database Tables 24

**Chapter No. Particulars Page No.**

**6 Implementation 25**

6.1. Modules and Modules Description 25

6.2. Technologies used 26

6.2.1. Java Database Connectivity 26

6.2.2. Requirements of use JDBC 26

6.2.3. JDBC Driver types 26

6.2.4. Microsoft Access ODBC Driver 27

6.2.5. Implementation of SHA-256 and AES encryption 28

6.3. Screenshots 31

**7 Testing 46**

7.1. Purpose 46

7.2. Dimensions of Testing 46

7.3. Types of Testing 46

7.4. Test Cases 49

**8 Conclusion and Future Enhancements 50**

**REFERENCES 51**

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig.No** | **NAME OF FIGURE** | **PAGE NO** |
| 1 | Time to crack Cryptographic Key versus Key size | 2 |
| 5.1 | Class Diagram | 15 |
| 5.2 | Use case Diagram | 17 |
| 5.3 | Activity Diagram | 19 |
| 5.4 | Sequence Diagram | 21 |
| 5.5 | State chart Diagram | 22 |
| 5.6 | Deployment Diagram | 23 |
| 6.1 | SHA-256 COMPRESSION FUNCTION | 29 |
| 6.2 | Block Diagram of AES Encryption and Decryption | 30 |
| 6.3 | Login screen of Password Wallet | 31 |
| 6.4 | Pop up box on not entering username | 32 |
| 6.5 | Pop up box if password field is empty | 33 |
| 6.6 | Pop up box if invalid username is entered | 34 |
| 6.7 | Home Screen of Password Wallet | 35 |
| 6.8 | Create Account Frame | 36 |
| 6.9 | If passwords don’t match while adding password to Password Wallet | 37 |
| 6.10 | Passwords successfully added | 38 |
| 6.11 | Modifying passwords | 39 |
| 6.12 | Deleting Passwords from Password Wallet | 40 |
| 6.13 | Confirmation for deleting password | 41 |
| 6.14 | Retrieving Passwords by entering the appropriate title | 42 |
| 6.15 | Changing Login Password | 43 |
| 6.16 | Forgot Password Frame | 44 |
| 6.17 | MAIN\_TB table in the database | 45 |

**LIST OF TABLES**

**Table No. Table Name Page No.**

1.1 Time to crack Cryptographic key versus key size 2

5.1 MAIN\_TB Table 24

5.2 UID Table 24

7.1 Test Cases 49