Secret Diary

Author: Bill BAO

1. Background

A diary has always been a particularly private thing for a person, which is why most people don't want to share it with others, or will only share it with a small group of people close to them. However, after surveying people around me who used to keep a diary, I discovered that most of them had their diaries watched or snooped on by their parents, which seriously discouraged them from keeping a diary and sticking to a good habit. This is overwhelmingly influenced by Chinese educational beliefs - such as that children should not have privacy, or that adults use the excuse of wanting to know more about them without respecting them. Based on the need to resist this invasion of privacy, I used my in-class knowledge of security and privacy to implement a secure diary, namely *It Keeps Secret*.

2. Technology

a) DES

The **DES** algorithm is known as the Data Encryption Algorithm (DEA). It is a bit-oriented and shared-key algorithm. They are based on 64 bits. In other words, each text—including plain text, encrypted text, and key—is split up into blocks, each of which is 64 bits. Although key should only be 8 bytes long, we could still obtain the key. The same key or password is used for both encryption and decryption. Encryption and decryption steps will be described briefly in the remaining paragraphs.

b) Hash Function

The National Security Agency created the cryptographic hash function SHA-1, which the National Institute of Standards and Technology (NIST) released as a Federal Information Processing Standard (FIPS). A message digest, which is produced using SHA-1, is a 160-bit (20-byte) hash value that is commonly shown as 40 hexadecimal digits.

3. Dependencies

commons-codec-1.15.jar
mysql-connector-java-8.0.30.jar

javafx

4. Features

User Features:

1. User could write diaries to record the title, weather, date, detailed content and a key that should be remembered (a diary, a key). Besides, the content has a variety of format to choose.
2. User could modify all diaries again, after firstly creating it, including the content and key etc. It is out of the concern that other people have known the former key, and user could change it again.
3. User could lock their diaries, so that even other people open this application, they still cannot see it.

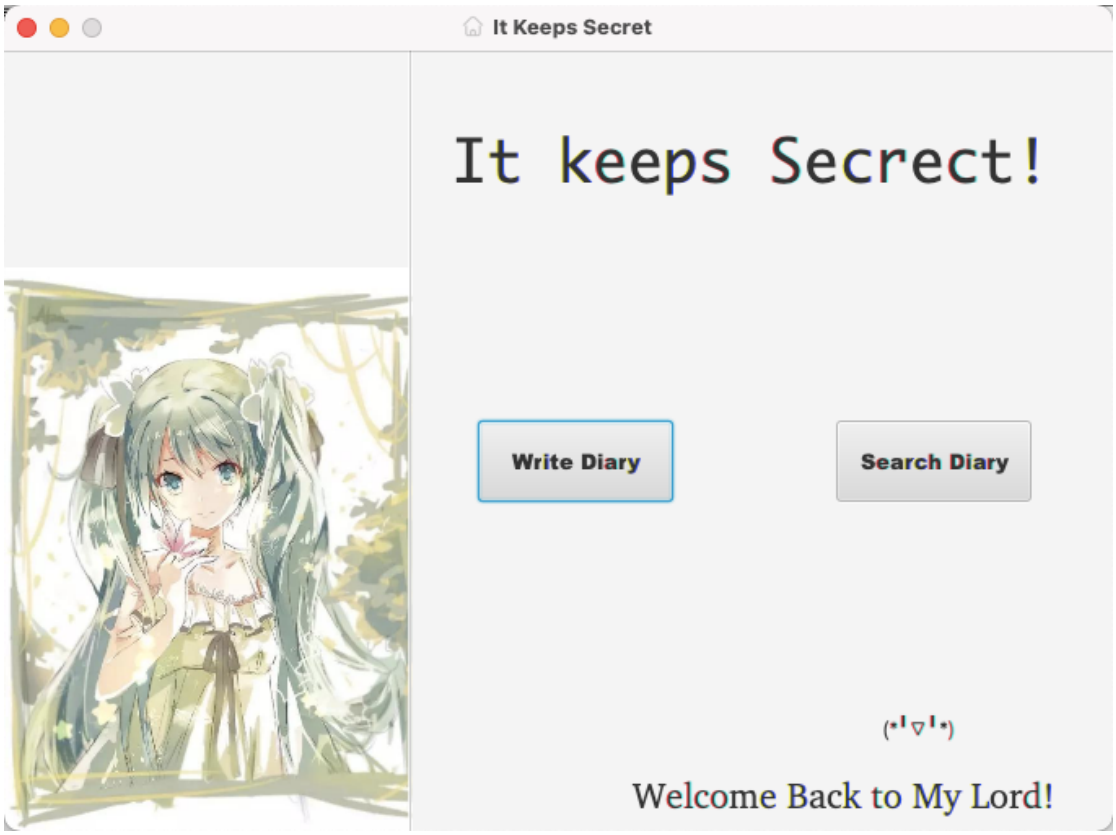
System Features:

4. DES algorithm is implemented correctly.
5. Even the database is opened, they still don't know the content. This is because the key is stored as a hashed value, and the content is encrypted before storing it.

5. User instruction

Since the database I use is MySQL, please create a local database called `secret`, and change the `mysql.properties` file to adopt your local database. Next, you could run the createTable.sql to create the `diary` table for storing your diary, and start your keeping diary journey.

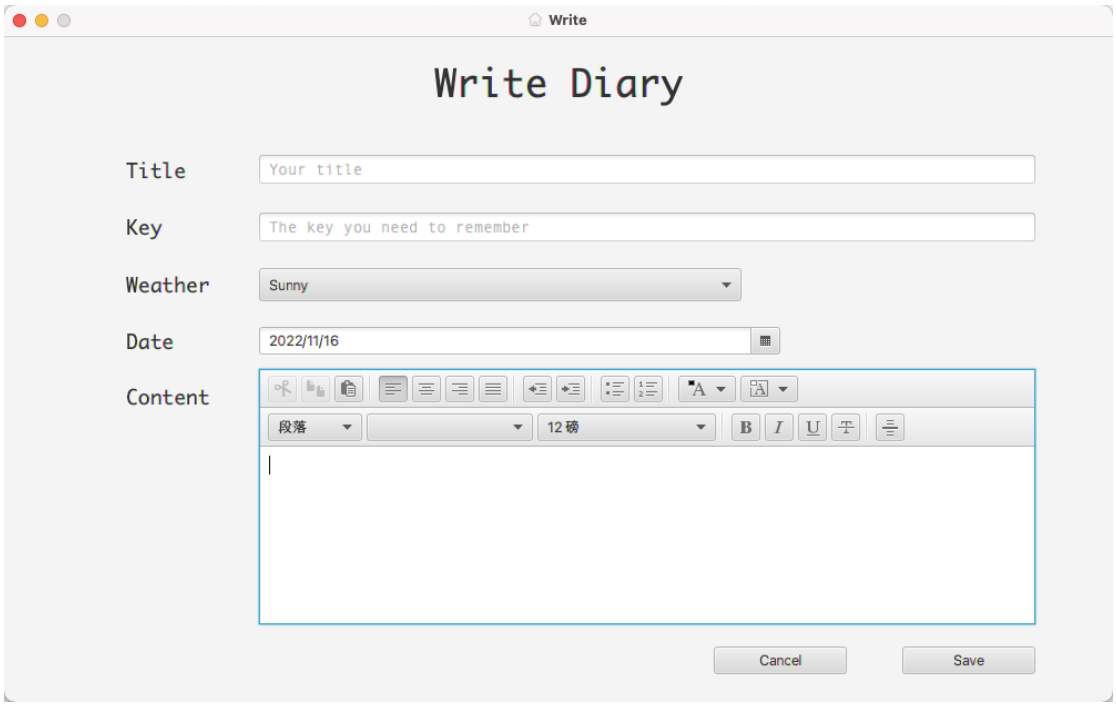
After above instructions, user could run the *DesApplication* file to open the main interface.



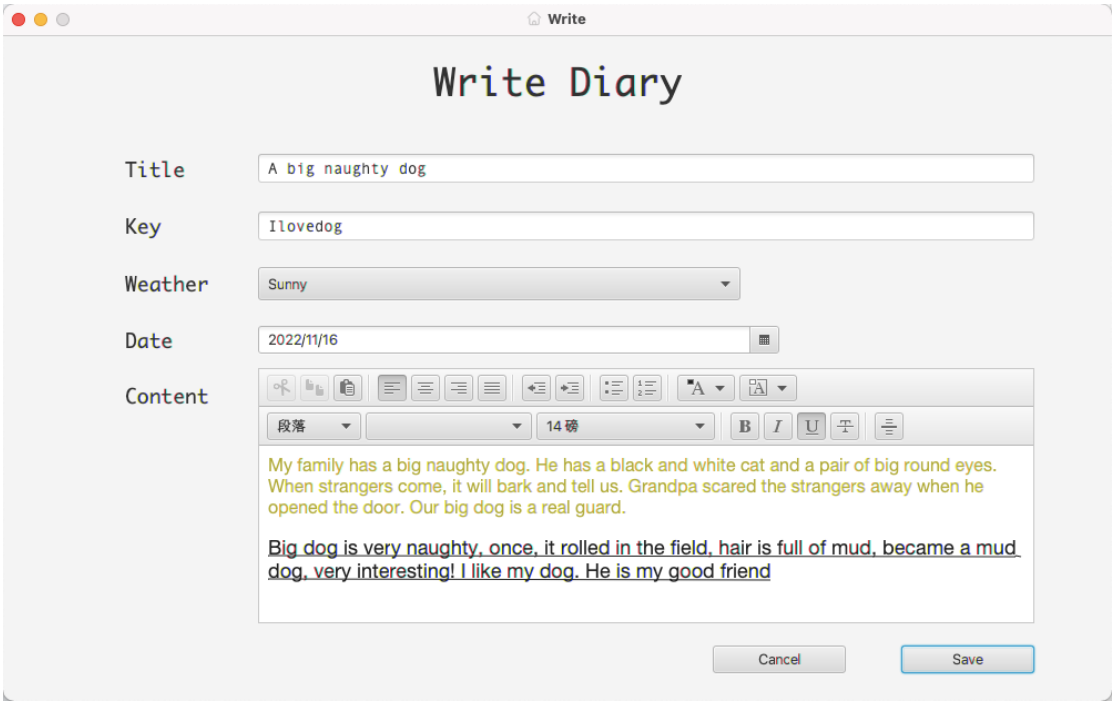
Next, user should choose the options that write diary or watch their diaries.

a. Write diary:

a) Click 'Write Diary' button



b) Enter anything that you want to record (**please remember your key**)

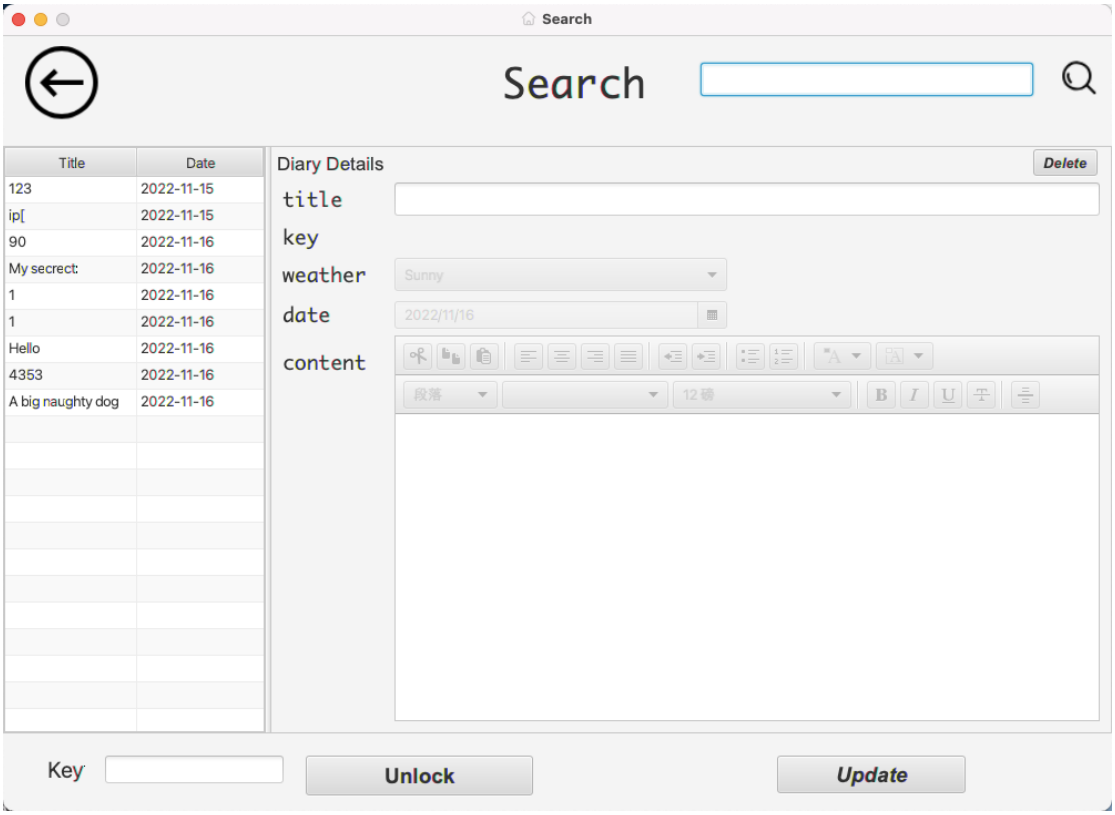


c) Click ‘Save’ button.

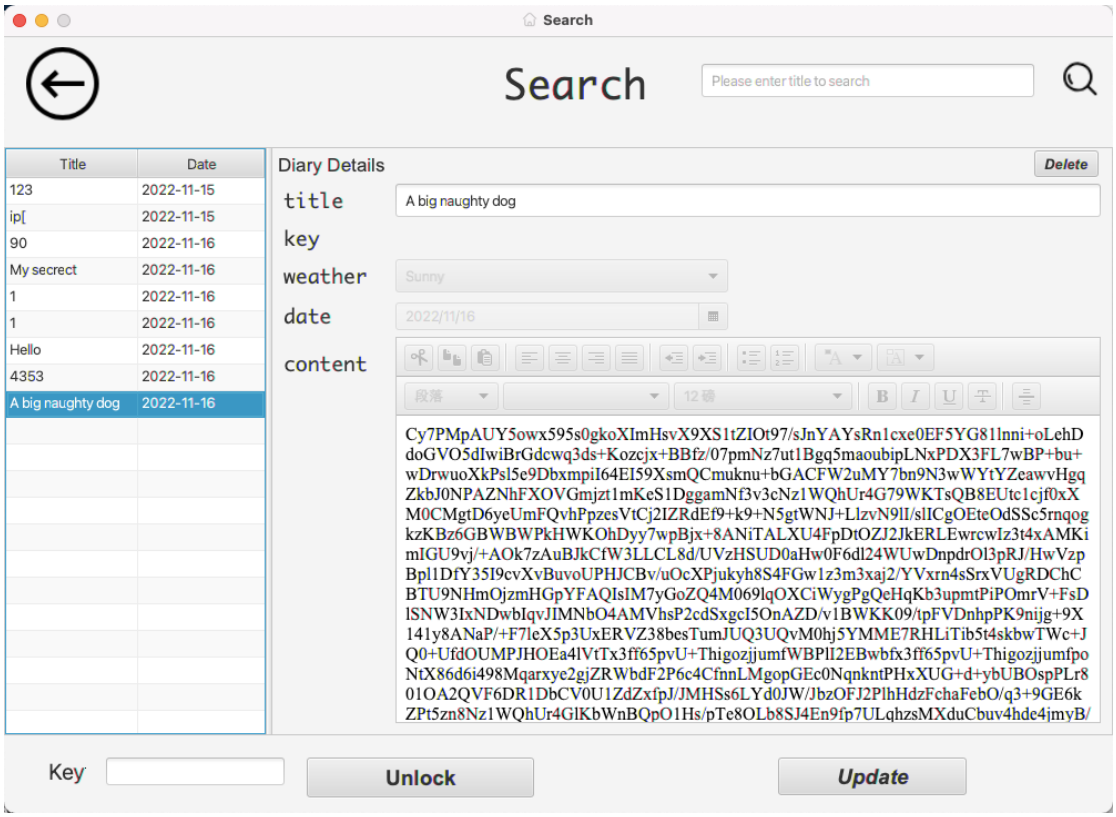
d) Then you return to the main interface

b. Modify diary:

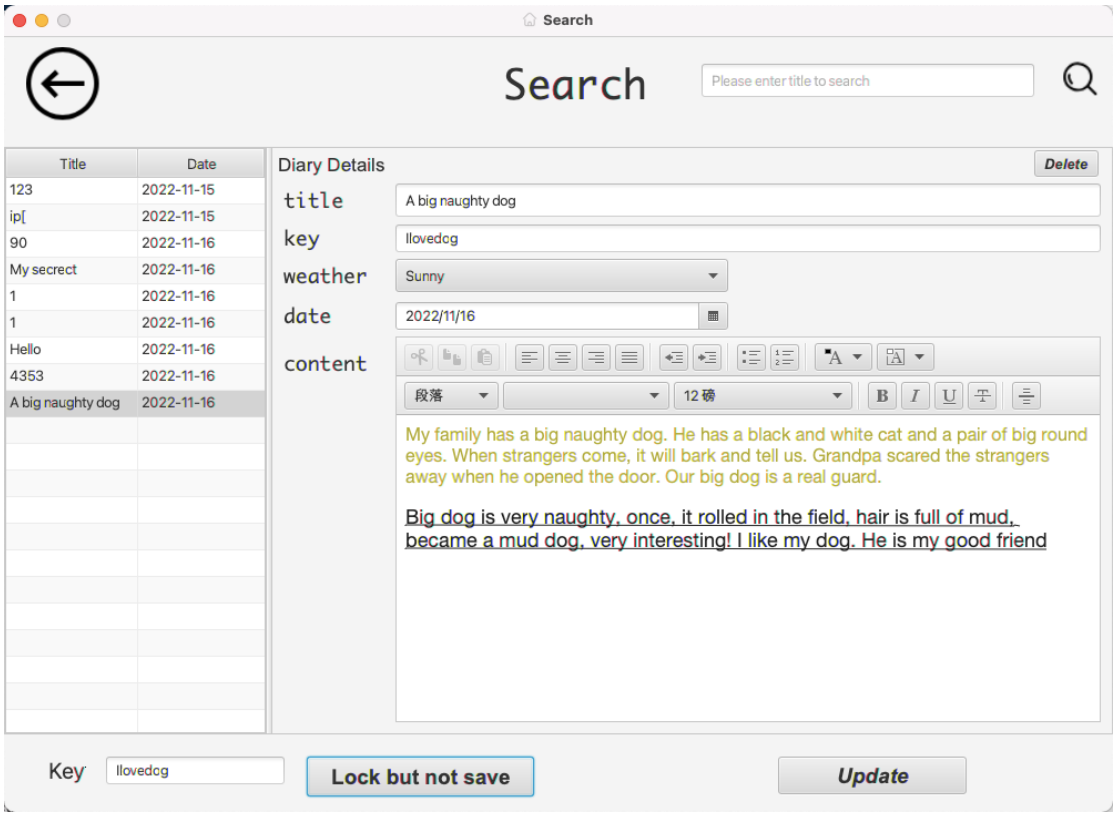
a) Click ‘Search Diary’ button, and you will see the diary you have written.



b) Select one of them at the right-hand side, but nothing you can see.



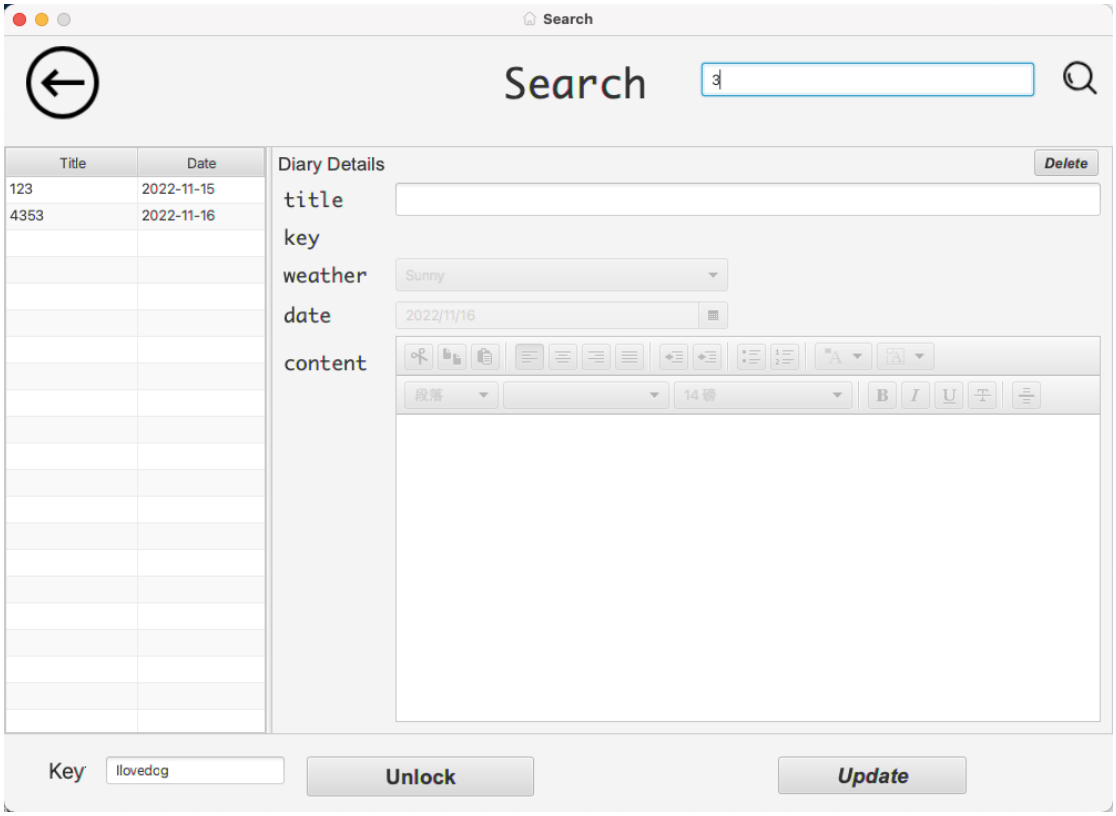
c) Enter key, and click ‘Unlock’ button.



d) User could modify as much as they want. Click ‘Update’ button to record the modification. Or click ‘lock but not save’ revert your modification.

c. Search diaries:

a) Use the title as keyword at the right top side, and Click the magnify icon to search all matching diaries.



b) Then do the **Modify Diary** again without the need to enter the view.