International Conference of Science, Engineering & Environmental Technology (ICONSEET), 3(24): 173-180, 2018
ISSN 0794-9650

www.repcomseet.com

Design of Folder Locker Application
A Case Study of C#.Net Application for Windows OS

Ekuewa J. B, Oyetunji O. O, Fabiyi A. O

Department of Computer Science, Federal Polytechnic, Ede, Nigeria

Abstract – Nowadays, most of computer users are facing problem for providing the security to the folder, so that it will not be accesses by the unauthorized user, sometimes folders are corrupted by the viruses which may in turn corrupt important files. Taking into consideration all these problems a model was designed which will provide the best security to folders and also save it from the viruses by using password authentication model. A Password based System was designed using alphanumeric password for securing it as a pass key, where the alphanumeric passwords were used for authentication process in this systems. These passwords are usually short and memorable that's why they can be easily guessed by the attacker, but strong system-assigned passwords are difficult to remember. This research provides security to folders with a platform independent environment, which is the bed rock of advanced economy; hence it's needs in a challenging economy.

Keywords: Alphanumeric, Authentication, Folder, Locker, Model, Password

---

1. Introduction

Because of the increasing threat to computer system, the information they store and process are valuable resources which need to be protected. Authentication refers to the techniques where users have to prove the claim of their identity to the identifier. There are many techniques through which users can be authenticated. Some of the password authentication techniques are knowledge based, token based, and biometric (Ferhaoui, 2010). Text password based technique and graphical password based technique comes under knowledge based authentication technique. A text password is a secret word or string of character that is used for user authentication to proven identity or for access approval to gain access to a resource. The easier a password is for the owner to remember generally means it will be easier for an attacker to guess (LI Fen et al. 2010).

However, passwords which are difficult to remember May also reduce the security of a system because, 1) a user might need to write down or electronically store the password, 2) users will need frequent password resets and 3) users are more likely to re-use same password. Unfortunately, these passwords are broken mercilessly by intruders. A graphical based password is one promising alternatives to textual passwords. According to human psychology, human brain can recall or memorize visual things better than texts. In graphical password based technique, sequence of images are used which are more memorable than sequence of characters. There are many graphical based password schemes available. Of interest are the cued-recall and click-based graphical passwords.

Locking folders is the best way to guarantee that nobody accidentally or intentionally gets access to your financial, health, private, and confidential information. Presently used password based systems have a number of associated inconveniences and problems such as user needs to remember passwords, passwords can be guessed or broken down via brute force and also there is problem of non-repudiation. Image password seems to be a better way out (Umut et al, 2009).

1.1 Problem Statement

With the advent of technology comes an increasing need for data and file security. Providing security to the folder is most challenging job for the developers. Information seekers tend to handle a system and

search through the system folders seeking for information from the system which can be used by them. Friends have turn out to be more of a treat than a friend, because the fact that you gave them access to your system, they explore it and made away with your vital credentials on the system. Therefore, the challenge of creating a folder locker need arise, and creating one with a secure and reliable source of authentication.

1.2 Research Aim and Objectives

The aim of this research is to develop an efficient folder locker application that will solve the problem of unwanted access to data and files.

The specific objectives are:

i. Develop a secure system folder locker
ii. Build a new algorithm for the security model of the folder locker application.
iii. Create a windows application for securing any folder with its contents, by setting a pass key for accessing that folder.
iv. Create an image authentication system.

1.3 Scope of the Study

This research work is centered on system application for security validation of folder access control and its content. Therefore, this study will work out only for the application which is a folder locker using an image model or alphanumeric passkey for validation means or authentication.

2. Research Methodology

The methodology applied in this research work is an Expert Systems Methodology (ESM). This method is best for security system and network solution software development (Sonia et al, 2009).

The primary data collection techniques used is:

i. Questionnaire
ii. Interview

Questionnaires and interview served as the primary means of gathering information for this research work. This method is a secured one out of all the method of data collection. The researcher felt that the use of questionnaire and interview would be the best way to gather adequate information for the research work and observation was used in order to present a meaningful project work.

The secondary data collection methods used involved gathering facts from:

i. Textbooks
ii. Journals
iii. Bulletin, and
iv. Newspapers

From the facts gathered, it was discovered that majority of computer users have issues with securing data and files. A popular but inefficient method most users adopt is by creating multiple folders inside folders, but with enough patience, an intruder will always get access.

2.1. System Architectural Model

The system architectural model encompasses different components of the system, technologies and concepts employed, which include, web services technology used to implement other service principles. SDLC principles and software project management techniques were engaged in the development process. Rapid Application Development (RAD) was used the software building process.

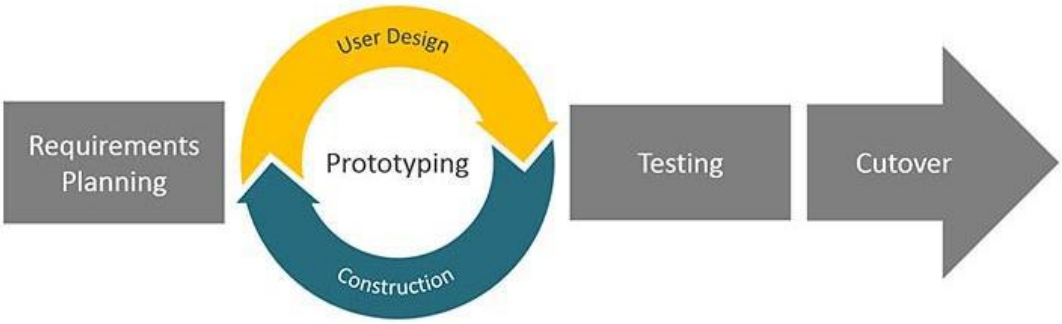

Fig1. Stages of the Rapid Application Development

With the RAD, we considered the following:

- Requirements planning phase – we combined elements of the system planning and systems analysis at this phase of the Systems Development Life Cycle (SDLC) as it is a generic standardized approach at this level. Discussions and approvals were made on business needs, constraints, project scope, and system requirements.
- User design phase –interactions were made users so as to meet their needs and also with systems analysts and we develop models and prototypes that represent all system processes, inputs, and outputs.
- Construction phase – We built the application at this phase with more focus on program and application. This covered programming and application development, coding, unit-integration and system testing.
- Cutover phase – A delivery of the built system was made at this phase.

The requirement specification entails adequately defining the functionality of a system and the functionality of the system however was placed in two categories:

- Functional requirements
- Non-functional requirements

2.2 Review of the Existing System

The major issue with the existing system is the loose access level of folders in the system. Folders are not protected; therefore, anyone that you give permission to your system automatically has access to all the folders and files in that system. This total made the existing system needs an upgrade or the development of a complete system to replace and solve the issues the previous system cannot solve.

2.3 Review of the New System

The new system allows locking of folders with a user friendly interface, securing files in folders, and requiring access key or access image to grant access to the specific folder. Hence the new system meets all this demand it was accepted as a replacement to the existing system.

2.3.1 Splash Screen

This is the first screen that comes on when the application is launched and while the application initialize or load its content.

Fig 2. Splash Screen

2.3.2 Login Page

This is the page where a user gets authenticated by inputting his/her passkey.

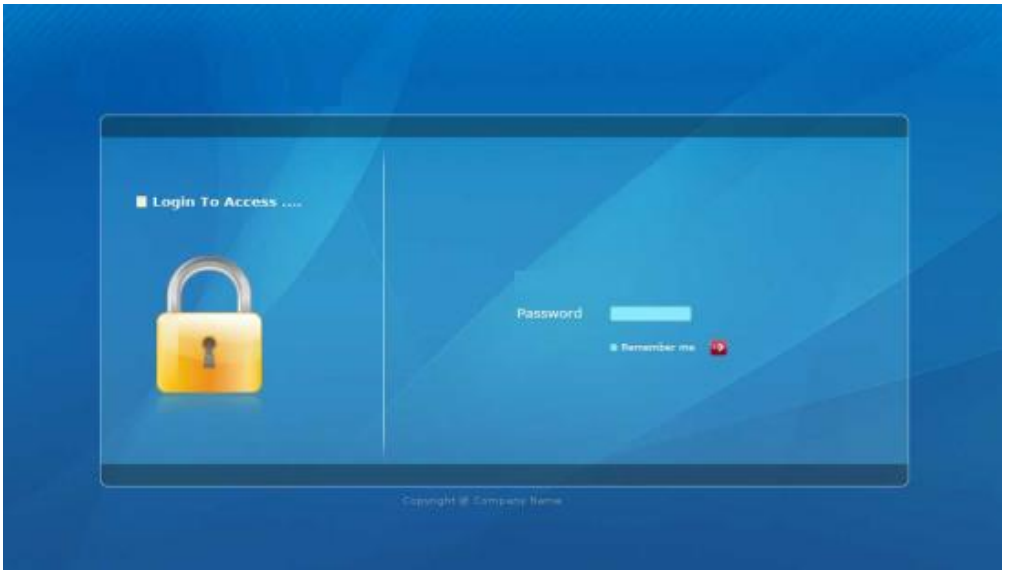

Fig 3. Login Interface

2.3.3 Main Screen

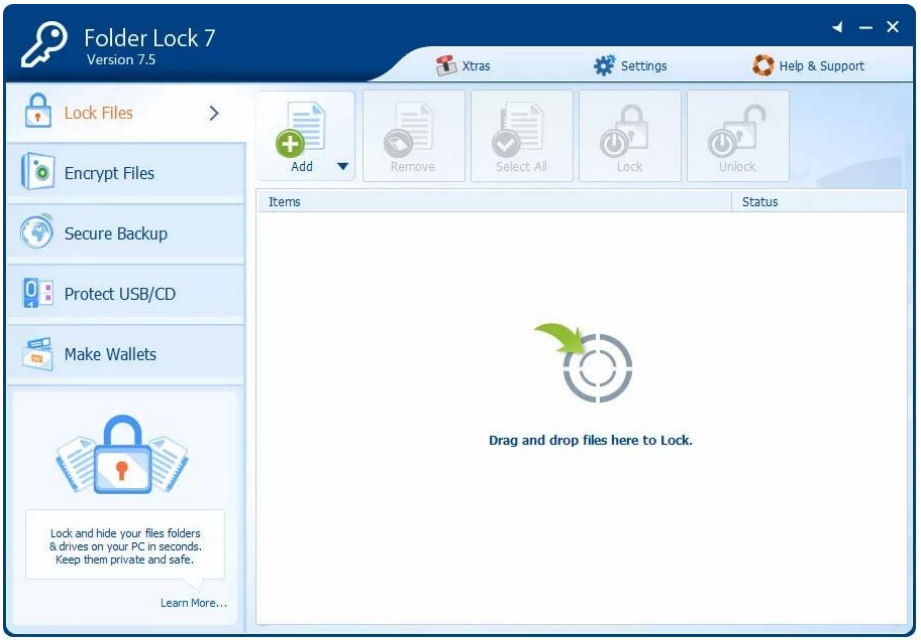

Fig 4. Main Interface

2.4 Sequence Diagram

The sequence diagram is a UML standard for presenting objects interacting with one another and it shows how each process interacts with the other and the order in which they interact. This illustrates how a user interacts with the system.

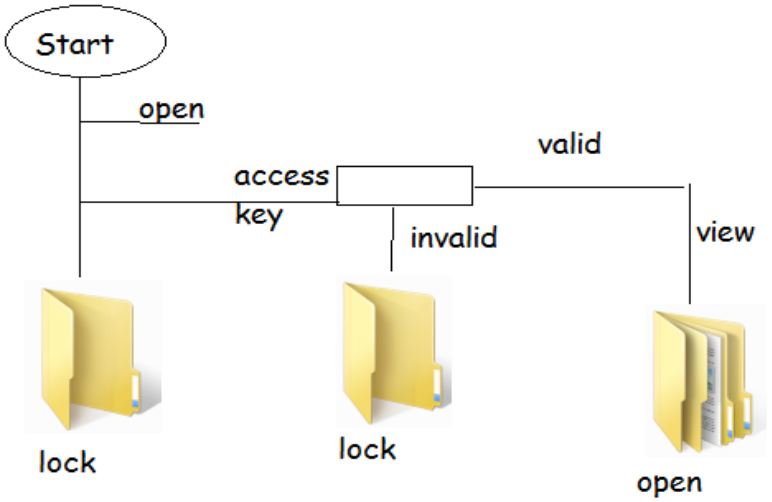

Fig. 5. Sequence Diagram

2.5 Data flow diagram

The Dataflow diagram shows you the sequential steps and procedure involved in the new system design and operation. The diagram below shoes the step for the flow diagram to lock or secure a files or folders in the system

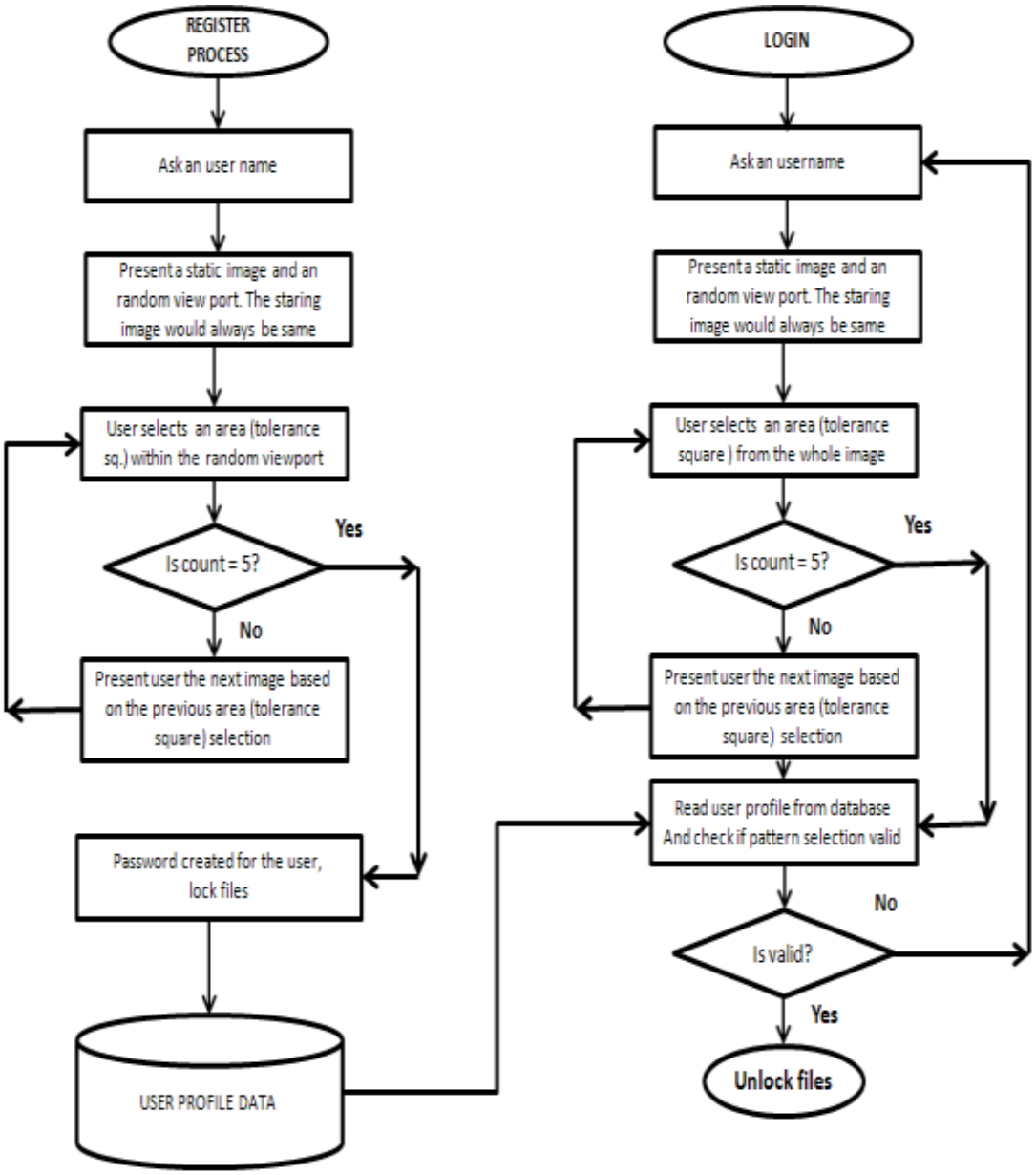

Fig. 6. Data Flow diagram

2.6 Information flow diagram

Information flow shows how to access a folder lock using this application. It is a three step operation to complete verification and open the folder.

Fig 7. Information Flow diagram

3. System Implementation

The system can be adopted using any of the following changeover methods as desired by the users:

- ✓ Direct change over: The new system is immediately and automatically adopted and all work operations would be switched instantly based on the working process of the new system
- ✓ Pilot change over: The switch over from the existing system to the new system is done in phases by deploying the new application gradually in modules or sections and evaluating the success and efficiency rate
- ✓ Parallel change over: The two systems (existing and newly developed) are run simultaneously over a period of time and best evaluations would lead to an appropriate full change over schedule.

4. Conclusion

The system lock folder was designed to hide a folder and encrypt a folder, which in the process of locking gives the user the permission to set his/her access key and confirm it, also unlocking the folder or having access to it, one will also be required to provide the access key which was set during securing time. Therefore, it can be said that the aim of the research is accomplished.

5. Recommendation

Having come to the completion of this design, it is recommended to every system user. And also to organizations and offices so as to secure there information and maintain their security and third party agreements.

References

Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. Van Oorschot. Persuasive Cued Click-Points: *Design, implementation, and evaluation of a knowledge-based authentication mechanism.* In IEEE Transactions on Dependable and Secure Computing (TDSC), (Oct, 2011)

K. Golofit. Click password under investigation. 12th European Symposium on Research In Computer Security, LNCS 4734, (Sept 2007)

S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, Springer, 8(6):387-398, (2009)

Sonia Chiasson , Alain Forget, Robert Biddle and P. C. Van Oorschot. Influencing user towards better password: Persuasive Cued Click- Points. *In Human Computer Interaction (HCI)*, The British Computer Society, (September, 2008)

Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, *An association-based graphical Password design resistant to shoulder surfing attack*, International Conference on Multimedia and Expo (ICME), IEEE. (2005)

P. C. Van Oorschot, A. Salehi-Abari, and J. Thorpe. *Purely automated attacks on passpoints-style graphical password.* IEEE Trans. Info. Forensics and security, vol. 5, no. 3, pp. 393-405, (2011)

Stobert, S. Chiasson, A. Forget, R. Biddle, and P. C. Van Oorschot. *Exploring usability effects of increasing security in click-based graphical password*. In Annual Computer Security Applications Conference (ACSAC), (2010)

LifangWua, SonglongYuana, *"A face based fuzzy vault scheme for secure online authentication"*, Second International Symposium on Data, Privacy, and E-Commerce. (2010)

LI Fen, LIU Quan, PANG Liaojun, PEI Qingqi *"Identity Authentication Based on Fuzzy Vault and Digital Certificate"* (2010)

UmutUludag, SharathPankanti, Anil K. Jain, *"Fuzzy Vault for Fingerprints"* (2010)

FerhaouiChafia, ChitroubSalim, BenhammadiFarid , *"A Biometric Crypto-system for Authentication"* (2010)