European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.55

ICONSPADU 2021
International Conference on Sustainable Practices, Development and Urbanisation

THE DEVELOPMENT OF A LOCK FOLDER APPLICATION WITH GRAPHICAL PASSWORD

Raznida Isa (a)*, Shuhadah Othman (b), Muhammad Zulhelmiy Fadlie Ismail (c),
Noor Maizatulshima Muhammad Sabri (d)
*Corresponding author

(a) Faculty of Computing & Multimedia, Kolej Universiti Poly-Tech MARA, Kuala Lumpur, Malaysia, raznida@gapps.kptm.edu.my
(b) Faculty of Computing & Multimedia, Kolej Universiti Poly-Tech MARA, Kuala Lumpur, Malaysia, shuhadah@kuptm.edu.my
(c) Faculty of Computing & Multimedia, Kolej Universiti Poly-Tech MARA, Kuala Lumpur, Malaysia, helmiy.fadlie@gmail.com
(c) Faculty of Computing & Multimedia, Kolej Universiti Poly-Tech MARA, Kuala Lumpur, Malaysia, shimasabri@kuptm.edu.my

Abstract

Nowadays, data protection is an essential issue for all computer users. Users continuously need to ensure that the data stored in their computers are secured. It became a significant concern for all computer users because cyber-crimes are constantly increasing day by day. In some cases, the situation turns out to be worst when their personal or confidential files being exposed and breached by an unauthorized user. It is risky when users probably will not distinguish the individual who attempts to access their confidential data typically stored in a folder on their personal computer or office desktop. Therefore, providing an extra security measure and protection to the laptop or specifically to the folder is the best solution, thus may prevent the folder from being breached by hackers. This project focuses on developing a lock folder application that implements a graphical password as its authentication factor to protect a folder from being accessed by an unauthorized user. It implements graphical passwords to verify user identity. Graphical password is an alternative authentication method that can replace a conventional password pattern where images are used in its authentication scheme. It will also send a notification via email if someone tries to unlock the folder without valid authorization. It has also been tested with users to study the user response towards its usability and functionality. The result shows the application is fully functioning and most likely benefit the user as it is user friendly and effortless to use.

Keywords: Graphical password, lock folder application, user acceptance testing

https://doi.org/10.15405/epms.2022.10.55
Corresponding Author: Raznida Isa
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

The rapid utilization and development of information technologies recently have made information security issue a primary concern to organizations and individuals. Most organizations commonly use information systems to operate their daily tasks and undeniably provide a personal desktop to their employees. As network and internet connectivity has provided significant benefits to modern society regarding sharing and accessing information, it also allows specific organizations to run smoothly. Nonetheless, security issues regarding confidential files are also on the rise lately (Basu et al., 2018). Unprotected files or folders on the personal desktop are at risk to be exposed and breach by an unreliable party. Therefore, it would be good to protect the files in a high level and trustworthy security system. Commonly to protect the document in the computer, the user will put extra security efforts into the computer. According to (Mahendran et al., 2018), providing additional safety measures for the devices may cause the overall system to become exhausted. The system will spend some time to secure all the data in the device unrelatedly to its status, either confidential or not. Therefore, it would be better if a system or application could specifically be tasked to protect folders and files. This kind of application is necessary to help user to protect their confidential files and folders. A lock folder application is said as one of the solutions that can be implemented to prevent private and confidential documents and folders from getting access by prohibited parties (Abdullah & Hamid, 2015). Only authorized users can access all the files and folders by using this kind of system or application. That kind of system required the user to enter their credential to verify their identity. Typical applications only need users to enter their registered passwords to enter the system. The application should encourage users to use strong and less predictable passwords for security purposes. Usually, the password-based system is preferable for most systems or applications that require user authentication. However, password-based systems have various related issues, such as users need to recall the password or others can easily guess the passwords. Otherwise, if users make a complex password, they might have difficulty remembering the password. For that reason, users tend to write down the password, users frequently reset the password, or users will use the same password repeatedly (Ekuewa et al., 2018). A password is a secret that the verifier and the user share. They are simply secrets provided by the user upon request by a recipient and are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists. Traditionally, alphanumeric passwords are used for authentication, but they have usability and security problems, as mentioned earlier. This paper has explained the development of the Lock Folder Application System with Graphical Password Login to protect the folders in personal computers from data theft or hackers. This application also will send a notification through email uses a simple mail transfer protocol if the folder has been unlocking by an unauthorized person. This application uses the image to replace the conventional password, which is called a graphical password. It is an alternative to an alphanumeric password. A sequence of pictures is used in a graphical password where it is easier to remember than the arrangement of characters. Additionally, this paper also will present the findings obtained after executing a user acceptance survey with a group of respondents.

The remainder of this paper is structured as follows. The following section discusses the previous works related to this project. The following section will explain the methodology used for this project. It will show the overall process that has been done to develop the project. Then the subsequent section will show the result gathered and depict the analysis based on testing made with the user. A discussion about the finding also has been made in this section. Finally, a conclusion is drawn to describe the achievement of this project and some recommendations for future research.

1.1. Literature Review

Authentication is a process of verifying a user's identity, device, or other entity in a computer system. It is a pre-requisite process to allow access to the resources in the computer system (Velásquez et al., 2018). Authentication ensures that only verified identities can log on to access system resources (Bhoyar, 2012). As time goes by, the technology in this world is slowly advancing to a whole new level. Nowadays, creators are fighting to build the most minor, slimmest phones and computers from huge, thick phones and computers (Jacobi, 2011).

Along with the advancement of technology, the internet is used more and more by everyone. Because of this, methods of authentication are required for these platforms. Almost every single web and person in this world has an online account to access something. Therefore, this will involve a password. A password is used as the central defence against crooks or attackers. Up until now, Password-based authentication is still widely used for online authentication on the internet and other systems. Password is still preferable to use because now the password is designed based on a password strength meter to help users pick a strong password to ensure the security level of the password (Golla & Dürmuth, 2018). It is just like how people letting their door unlocked led to a burglary or theft. There is some personnel information about users that the web or company needs to use or the users themselves.

Generally, nowadays, the increasing threat to the computer system and the information they store and process are valuable resources that need to be protected. Authentication refers to the techniques where users must prove the claim of their identity to the identifier. There are many techniques through which users can be authenticated. Some password authentication techniques are text passwords and sending a notification in the user's email to discover that their application is being hacked. The primary purpose of this project is to prevent shoulder-surfing attacks, key-logger exploitation, and password cracking issues by using an adaptation of the pass faces scheme with added direction. This project also is evaluated and compared to demonstrate the security strength and robustness. However, this paper only discusses the user acceptance feedback after testing this application.

Using a password is a common practice for user authentication. Users need to memorize the password, and it can still be considered safe as long as only the users know the password. However, in reality, the passwords cannot always be kept safely as the human brain cannot manage passwords for many services at once (Erdem & Sandikkaya, 2019). A text password is a secret word or string of characters used for user authentication to prove 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. However, passwords that are difficult to remember may also reduce the security of a system. Because users might need to write down or electronically store the password, users will need frequent password resets, and users are more likely to reuse the same password. Unfortunately, intruders break these passwords mercilessly by several simple means: masquerading, eavesdropping, shoulder surfing, and social engineering attacks.

Therefore, this project will implement a graphical password authentication during user login to the application. Graphical passwords use pictures (also drawings) as passwords. Graphical password systems is a promising alternative of text-password in academic research area and industry. Graphical passwords use system image recognition such as faces, uploaded images, recalling a sequence of actions such as clicking and drawing (Yu et al., 2017). The graphical password was invented by (Blonder, 1996). It deals with one image that would appear on the screen, and then the user would click on few chosen parts of the image. Technically users need to click on a few chosen regions within the image.

After the user successfully clicks the correct region, the user will be authenticated. When using a graphical password, users are required to select a memorable image. A user needs to choose a memorable image because meaningful content can support memorization (Lashkari et al., 2010). Nowadays, it is crucial to keep secure private data. Both students and lecturers may be saving passwords or login information in the documents folder, or have files that are confidential for others, or files with valuable information that can be stolen or lost. Important files and folders like this need password protection so that intruders or unauthorized users cannot access, read, view, copy, and move or delete them. By having notification in the software, it can be hard to hack by any hackers. So, users are will not having any problem if they already locked their files and folders. The creation of the graphical password will somehow or somewhat be helping on improving the security of a password. As said earlier, the percentage of users forgetting their texts are lesser.

A folder lock application is one of the solutions used to ensure nobody intentionally gets access to private and confidential information. The existing project has shown that the lock folder application is a significant project that can help computer users to protect the folders in their personal computers. A project published in (Mundhra, 2015) shows that a lock folder application is one of the must-have applications computer users need to install on their PC. The applications provide many features for the user to use to protect the confidential folders. This application will ask users to set the master password as a security authentication. According to the manual application, users need to remember the password precisely and not forget it at all. If the users forget the password, the application cannot retrieve the password back, and the user will not ever get to access their file back. This situation is risky because people have a high tendency to forget the password, as discussed previously.

Due to the limitations of the existing project, the project tries to cast a deeper look into users who have trouble remembering their passwords and locking their folders. This Lock Folder Application System with Graphic Password Login will help users who forgot their password by using two-factor authentication to recover the password. The app will give the user a security question, and the user must answer the question correctly. In addition, the purpose of this security is to prevent files or applications from being compromised by hackers. The app can send a notification alert to the user if someone or a hacker unlocks a file or document without permission. The notification will be sent to them via email.

https://doi.org/10.15405/epms.2022.10.55
Corresponding Author: Raznida Isa
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

2. Problem Statement

Information seekers or hackers tend to explore a system and search all the system folders seeking information to abuse or manipulate. Computer users are at risk of exposure to this threat due to any reason. Some people are unaware their computer is not logged out before leaving the desk. The project is developed because unprotected files and folders can lead to theft, data loss, and privacy breaches. This situation relates to the purpose of this research as to identify the effectiveness of the lock folder application system. Another reason is that most computer users have a minor security system on their computers. When they create a password, they prefer to use things that have meaning to them to be easier to remember. Hackers can guess the predicted password and access their computers freely. The currently used password, the text and alphanumeric password, is still a robust authentication method. However, because of the advancement of technology, there has also been a rapid increase in hacking cases. Therefore this application will implement a graphical password to ensure the security and of the folder lock application is more robust and reliable.

3. Research Questions

Based on the background study and problem statement, this study proposes the following research question which are:

i. Why is it essential to protect our data in a computer folder?
ii. How is a graphical password more effective than a conventional password?

4. Purpose of the Study

This study aims to develop an application that gives complete protection for a folder on a personal computer. Using the graphical password as an authentication factor may surge the protection level to prevent users from becoming data theft victims. The application could also provide notification via email if the folder is attempted to be attacked by hackers.

5. Research Methods

This project uses Waterfall Model Methodology as its project development strategy. This methodology is chosen because it is easy to follow and suitable for a small project. The verification at each stage can help early detection of errors or misunderstandings. It is a linear sequential flow methodology. The progress will be seen as flowing steadily downwards (like a waterfall) through the phases of software implementation. This methodology breaks the project into multiple phases, where each phase is started when the previous phase is complete (Kramer, 2018). The phases start with the requirement phase, where all the requirements are identified and analyzed. The requirement phase mainly focuses on the task where we supplied a questionnaire to the users to identify the necessities for this application. Then we also gathered data thru interview users directly with the meeting and discussion. Then, it continues with the design phase, where the infrastructure and the system's interaction are organized and designed through diagrams or blueprints. Next, the coding phase will proceed, where the

https://doi.org/10.15405/epms.2022.10.55
Corresponding Author: Raznida Isa
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

system will be developed according to the plan structured in the design phase. After the development is finished, the system being tested. The testing phase aims to further search out defects within the system to verify whether the appliance behaves evidently and in line with the requirements analysis. This cycle is repeated until all requirements are tested and every error and defect is fixed. Eventually, the application system can be deployed after the testing phase is successfully done.

5.1. System Architecture

The system's flowchart diagram is shown in Figure 1. The system begins with the user's sign-in. The user can then log in using the system. After entering the username and graphical password, the user must click Login. Following that, the PC will display the lock folder's menu page. The user must select the folder that they want to lock. The user must then upload a folder that has been locked or unlocked. Finally, the user has the option to log out of the system.

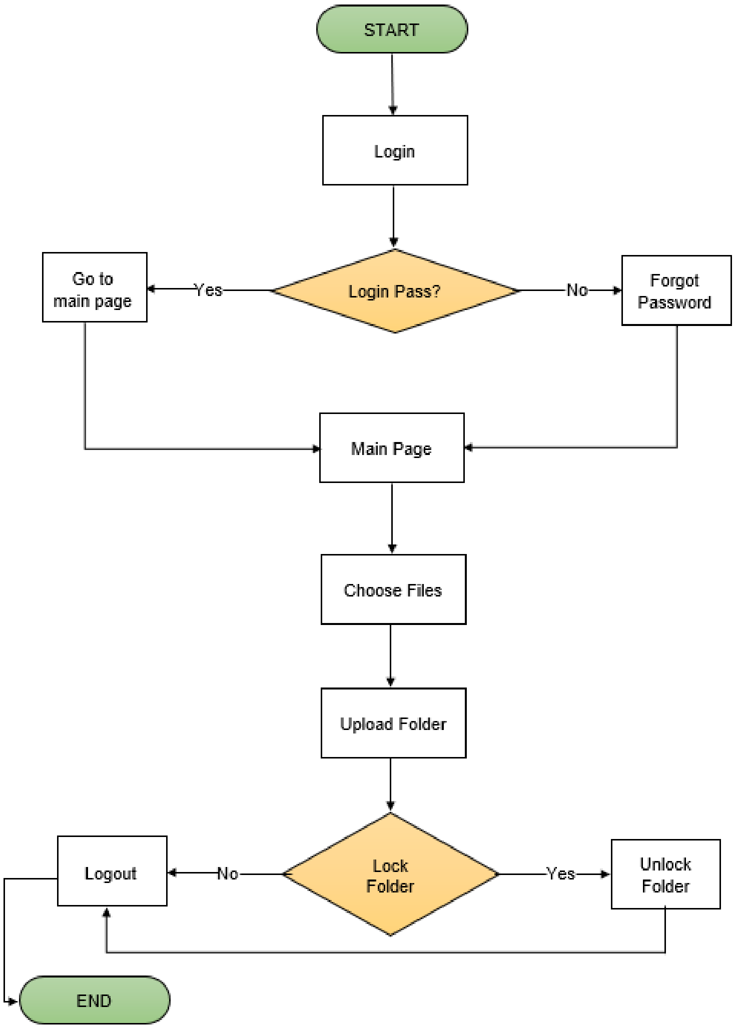

Figure 1. Flowchart diagram

The Lock Folder Application System's flow diagram is shown in Figure 2. The main flow begins with the application software being run. When the user forgets his or her password, log in to the software using a recovered password. Then, go to the main page of the server's lock folder that can be accessed. Users can execute a variety of actions or activities, such as login, lock folder, and unlock folder, all while watching the loading bar progress. After that, if the user unlocks the locked folder, an email will be sent to them.

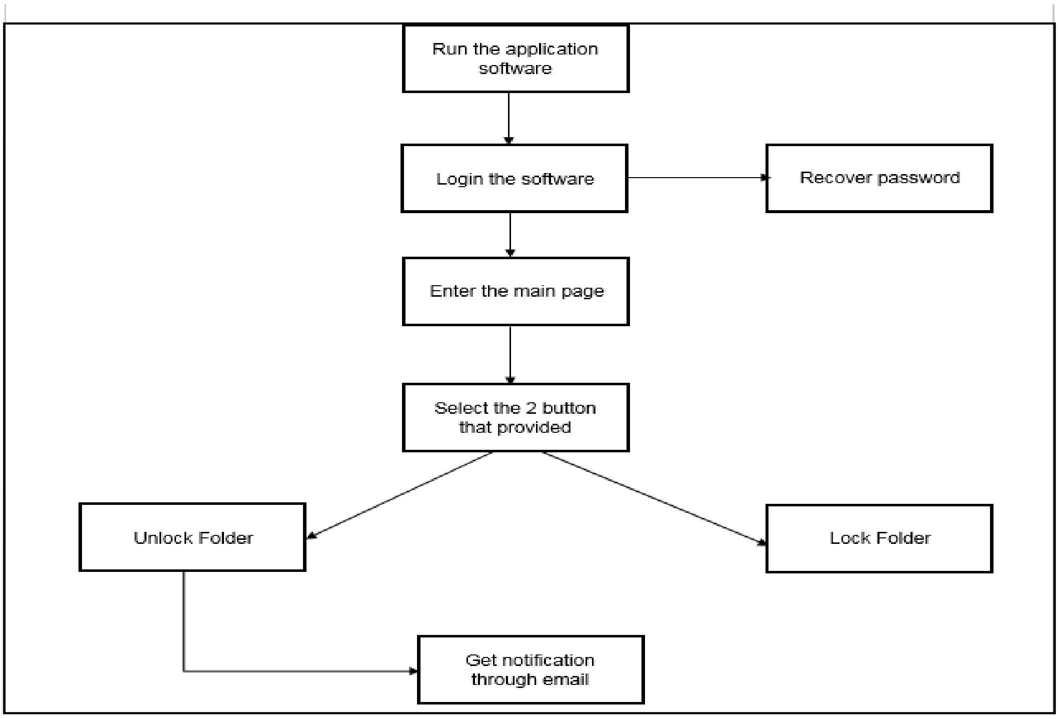
Run the application software
Login the software
Recover password
Enter the main page
Select the 2 button that provided
Unlock Folder
Lock Folder
Get notification through email

Figure 2. The flow design of folder lock application system

6. Findings

This section presents the result of the user feedbacks obtained from user acceptance testing. Application has been tested to the selected respondents, and the feedback has been analysed appropriate manner.

6.1. User Acceptance Testing

A qualitative research approach for this study was chosen because qualitative methods are relevant to see how users respond or feel about the system's functionality. User acceptance testing was done on 50 respondents that involved students and staff in Kolej Universiti Poly-Tech MARA. The purpose of the acceptance test is to decide if the proposed application meets all the requirements that have been determined and produce the expected output. It is a conventional test that is conducted with the clients. The client needs to decide if the system fulfils its acceptance criteria and to allow them to decide whether to accept the system or not (Suman & Sahibuddin, 2019). In this project, the respondents require to answer a questionnaire. It consists of a set of questions about the features and the functionality of the

https://doi.org/10.15405/epms.2022.10.55
Corresponding Author: Raznida Isa
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

system. Table 1 shows the overall results from the testing. All the feedbacks are scaled at the following rate: poor, fair, good, and very good.

There are ten questions prepared in the questionnaire. The first three questions asked the respondent about the application's appearance, such as the font used, the layout, and the overall background of the application. Average 43.1% respondent choose very good, means most of them can accept the application's look. The following questions asked the respondents about the features includes in the applications. The graphical password login is working correctly as 41.5% of respondents answers good. The application provides a few menus for the users to choose such as menu lock or unlock the folder. 41.5% of respondents agreed that the menu is appropriate and functions accordingly. Next, 36.6% choose the menu to retrieve the password if forgotten is working correctly. Furthermore, most of the respondents agree that the application is compatible with their system computer. The application completes the main task, which is to lock and unlock the folders. Finally, most respondents agree to use this application on their computer as the application is secured to be used. Overall, we can summarize that the application meets user satisfaction and users agree that the application's primary purpose is successfully achieved.

Table 1. Testing result

No.	Question	Scale and percentages			
		Poor	Fair	Good	Very Good
1.	The font used in this application is suitable and readable	0%	22%	36.6%	41.5%
2.	The layout of this application is easy to use	2.4	24.4	31.7%	41.5%
3.	The background of this application is simple and adequate	0%	19.5%	34.1%	46.3%
4.	The graphical password login is working properly	0%	19.5%	41.5%	39%
5.	The menu page (to lock or unlock) on this app functions properly	2.4%	17.1%	39%	41.5%
6.	Forgot Password on this app is working functionally	4.8%	24.4%	34.1%	36.6%
7.	This application is compatible with the system computer	0%	24.4%	41.5%	34.1%
8.	The app successfully manages to lock and unlock the folder	0%	19.5%	46.3%	34.1%
9.	Password user has been encrypted, and it secured	0%	26.8%	36.6%	36.6%
10.	Are you ready to use this app on your laptop in future	0%	17.1%	39%	43.9%

The second result is for the functionality of the application. Functional testing is a software testing process to test all the functions provided in the system or application. The purpose of this testing is to ensure the system are well functioning and meets the requirements. Besides that, Functional testing is a way of checking software to ensure that it has all required functionality that's specified within its functional requirements. All function in the lock folder application has been tested, and the result is obtained as shown in table 2.

Table 2. Functional testing result

Function	Expected Result	%	Status
Login	Users will be able to log in to the system with the username password provided.	100%	Working Properly
Forgot Password	Users will be able to select an item from the question and get the answer.	100%	Working Properly
Lock	Users will be able to lock their folders with straightforward and efficient.	100%	Working Properly
Unlock	Users will be able to unlock the folder and get an email from the software.	100%	Working Properly
Change Username and Password	User can be changing their username and password.	100%	Working Properly
Account	Users will be able to select their questions and save them for recovery password.	100%	Working Properly

7. Conclusion

This Lock Folder Application software is developed to help user to keep their files in a safe place. The development of the Lock folder application system with graphical password login is successfully implemented according to the planned and predetermined time. In this application, we provide the user with a new way to verify the owner's file and folder identity. Other than that, users also will receive a notification via email after they unlock the folder to maintain the stability and security of the application software. User’s feedback has shown that this application system has successfully functioned according to user requirements. There are some limitations for this Lock Folder Application: the application cannot be used for a single or an individual file outside the folder. It has to be inside the folder so that the folder can be locked. The file that has been locked in the folder has no secure backup in the server. More features to be included, such as making locked files encrypted, making the folder invisible, and file shredding features that make deleted files cannot be recovered anymore. The Lock Folder application will be equipped with more advanced features in terms of its use and security for future work. The application will be upgraded with proactive notifications like a quick message through phone, and the application will securely backup the folder through cloud storage.

Acknowledgements

The authors gratefully acknowledge Kolej Universiti Poly-Tech MARA Grant URG/0520/FCOM/FP1318 (10) for providing financial support. The authors also would like to thanks all the team members involved for their contribution.

References

Abdullah, N. B. Y., & Hamid, H. R. B. M. H. (2015, October 1). Folder Lock by Using Multimodal Biometric: Fingerprint and Signature Authentication. *IEEE Xplore*. https://doi.org/10.1109/CyberSec.2015.35

Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., & Sarkar, P. (2018, January 1). Cloud computing security challenges solutions-A survey. IEEE *Xplore*. https://doi.org/10.1109/CCWC.2018.8301700

https://doi.org/10.15405/epms.2022.10.55
Corresponding Author: Raznida Isa
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Bhoyar, K. N. (2012). Biometric Folder Locking System using Fuzzy Vault for Face. *Semantic Scholar*. https://www.semanticscholar.org/paper/Biometric-Folder-Locking-System-using-Fuzzy-Vault-Bhoyar/f844017fae910a9e269950553d69cb5c40c41170

Blonder, G. E. (1996). Graphical Password. *Google Patents.* (Washington, DC: U.S. Patent and Trademark Office Patent). https://patents.google.com/patent/US5559961A/en

Ekuewa, J. B., Oyetunji, O. O., & Fabiyi, A. O. (2018). 'Design of Folder Locker Application A Case Study of C#.Net Application for Windows OS', *International Conference of Science, Engineering & Environmental Technology (ICONSEET), 3*(24), 173-180.

Erdem, E., & Sandikkaya, M. T. (2019). OTPaaS—One Time Password as a Service. *IEEE Transactions on Information Forensics and Security, 14*(3), 743–756. https://doi.org/10.1109/tifs.2018.2866025

Golla, M., & Dürmuth, M. (2018). On the Accuracy of Password Strength Meters. CCS '18: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1567–1582. https://doi.org/10.1145/3243734.3243769

Jacobi, J. L. (2011, December 27). Hide and Secure Data With Folder Lock. *PCWorld*. https://www.pcworld.com/article/247068/folder_lock.html

Kramer, M. (2018). Best Practices in Systems Development Lifecycle: An Analyses Based on the Waterfall Model. *Review of Business & Finance Studies, 9*(1), 77–84. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131958

Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. *Scientific Research and Essays, 5*(24), 3685–3975. http://www.academicjournals.org/sre/PDF/pdf2010/18Dec/Lashkari%20et%20al.pdf

Mahendran, D. R., Jamal, A., Helmi, R. A. A., & Aisha, M. (2018). Trusted computing and security for computer folders. *International Journal of Medical Toxicology & Legal Medicine, 21*(3&4), 83. https://doi.org/10.5958/0974-4614.2018.00036.0

Mundhra, A. (2015, April 23). How to Use Folder Lock on Windows to Lock, Secure Files. *Guiding Tech*. https://www.guidingtech.com/42212/folder-lock-windows/

Suman, R., & Sahibuddin, S. (2019). User Acceptance Testing in Mobile Health Applications. *Proceedings of the 2019 2nd International Conference on Information Science and Systems*. https://doi.org/10.1145/3322645.3322670

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology, 94*, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security, 70*, 179–198. https://doi.org/10.1016/j.cose.2017.05.006