KEMENTERIAN PENDIDIKAN TINGGI

JOJAPS

eISSN 2504-8457

POLITEKNIK MALAYSIA PORT DICKSON

Journal Online Jaringan COT POLIPD (JOJAPS)

# The Use of *SecUrAccess* Software to Protect Information Stored In a Computer

Jacey Mariadass[a]*

[a]*Tel:012-5250603 Fax: 05-5471162 E-mail: jacey2606@gmail.com*
*Politeknik Ungku Omar, Jalan Raja Musa Mahadi, 31400 Ipoh, Perak Darul Ridzuan*

**Abstract**

Information has great importance for any organizations and should be adequately protected especially information stored on a computer. Physical security is considered as a part of information systems security. Small devices such as USB flash drives via USB ports are sometimes allowed in organizations. Due to its small size, low cost and large storage capacity of USB flash drive, the usage is very demanding for storage purpose. Therefore, data storage without adequate operational and logical controls can pose a serious threat to information confidentiality, integrity, and availability (CIA). The use of USB flash drives can; (i) increase the risk of data theft (when there is no control on copying information from a computer), (ii) data loss (when a physical device is lost) and (iii) data exposure (when sensitive data is exposed to third party without consent). The idea to develop *SecUrAccess* software is to keep the information stored in user's laptop or computer from being transferred to USB flash drive via USB port. This software can minimize the data theft incident and virus infection by not allowing unauthorized users to plug their USB flash drive. The authorized user needs to define a USB access rights policy to make these USB flash drive write protected or not in order to be accessed through the system. In term of security purpose, the user is required to enter a password each time to change the policy. The software is equipped with a high level of security. Whenever an unauthorized user enters the wrong password three times, the computer will log off automatically. The software is fully developed using Microsoft Visual Studio Ultimate 2010. Overall, the feedback result shows majority respondents agreed on the effectiveness of *SecUrAccess* software and are satisfied with the software.

*Key-word: Information, data theft, unauthorized user, access rights, risks*

## 1. Introduction

The increased use of portable devices causes new security concerns. This is due to its robustness, size and weight which makes them easy to carry, unfortunately, there is a high risk of losing or misplacing. Data security has risen to be one of the highest concerns for computer users. Removable media causes problems to an organization since insiders can use such media to remove proprietary information from company systems (Silowash & King, 2013). Insiders may do this for legitimate reasons, such as to work on material at home, or they may do so for malicious reasons, such as to steal intellectual property. Cybercriminals and data thieves are using removable media to introduce malware and steal information from computers. Besides that, data loss through the misplacement of an unencrypted device is also highly reported. Although USB storage devices offer many advantages for us, however, at the same time, they cause security problems because it is easy to copy files to a USB drive in few seconds. According to Widya et. al. (2011), a user might have confidential data inside their computer which user does not want others to copy through the USB drive. The large storage capacity of USB flash drives and low cost means that by using them for data storage without proper security protection can pose a serious threat to information confidentiality, integrity and availability. The widespread use of USB flash drives within an organization can expose to data loss on two major fronts which are data stolen by copying onto a drive and data were stolen using the drive to copy from a computer. Most organizations are aware that a computer information system serves as a backbone of their establishment, in which users must be aware of the threats that might occur (Cooper, 2017). This is to minimize the risks of information systems and breach of information to the third party. Theft in cybercrime may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information (Brown, 2015).

Organizations must establish and implement effective methods and processes to prevent unauthorized use of removable media while still allowing users with a genuine business to use the flash drives. A policy-based solution should allow different rules to be applied to USB ports. When a laptop or other computing device is in a riskier environment like an airport, policies can be set to restrict all USB connections. When the device is inside the company's walls, read and write access might be permitted. In other locations, like user's home, read-only access might be applied. Due to that, it is a need to define a USB connection either to enable or disable the USB port to be accessed through the system and at the same time user can still use their USB port to plug in their mouse and keyboard although USB connection is disabled. Where else for USB access rights policy, it should define either the user can read only or read and write. There are many options where changes can be done in the registry of the computer to prevent USB storage drivers when the system boots, not everyone has the access rights to do so. This is because changes in the registry will corrupt the user's computer (Darin, 2015).

Therefore, the purpose to develop *SecUrAccess* software is to keep data secure in user's laptop or computer which is convenient, user-friendly and can be installed easily and used by all level of the user. This software provides secure data on computers which disables unauthorized users to copy data using USB flash drive via USB port. *SecUrAccess* software will be developed according to the objectives that have been identified; (i) to develop *SecUrAccess* software for computers and laptops, (ii) to enable or disable USB port from being used to insert USB flash drive, (iii) to define USB policy either to read only or read and write and (iv) to log off user's computer automatically if wrong password is entered three times.

The scope of this work is to ensure that the objectives of this project can be implemented successfully in real life. A number of system scope and user scope were listed in order to ease and produce clearer instructions to the users. The focus of this software is for all levels of a computer user. The purpose of developing *SecUrAccess* software is to protect data theft and at the same time protect the computer from virus which is being transmitted through USB flash drives via USB port. The user only needs to define a USB connection to enable the USB drives or disable the connection using the software. Besides that, it can also help the management of any organization or user themselves to protect their information in their computer from being accessed by an unauthorized person. The significance of this software is, it's user-friendly. It gives the advantages for computer users since this software support Windows.

## 2. Methodology

The *SecUrAccess* software is developed by using Microsoft Visual Studio Ultimate 2010. Waterfall model was selected as it is sequential and linear which serves the purpose of the system that was developed in which progress is seen as flowing through the phases of (i) requirement definition, (ii) system and software design, (iii) implementation and unit testing, (iv) integration and unit testing, (v) operation and maintenance (Sommerville, 2011) as shown in Figure 1.

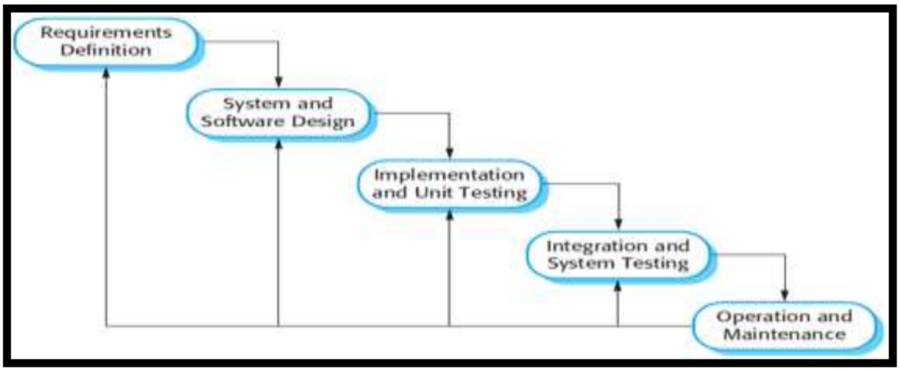

Requirements Definition
System and Software Design
Implementation and Unit Testing
Integration and System Testing
Operation and Maintenance

**Figure 1** Waterfall Model / Software Life Cycle
Source: Adapted from Sommerville (2001, pg.45)

In the requirement definition phase questionnaire is carried out to understand the needs and problems. The information that was gathered is analyzed and implemented in the project. During system and design phase, the conception of *SecUrAccess* software was sketched (refer to Figure 1) and all the requirements are converted into system design. In implementation and unit testing phase, inputs from system design are used to develop small programs called units, which are integrated into the next phase. In integration and system testing, testing the software against requirements and use cases are done. It also includes fixing the defects found as determined by the software testing life cycle. In operation and maintenance phase, the software was tested randomly among the computer users to ensure that any issues which arise during the operation were solved and to make sure the software can function and run smoothly. Maintenance is done to deliver these changes in the user environment.

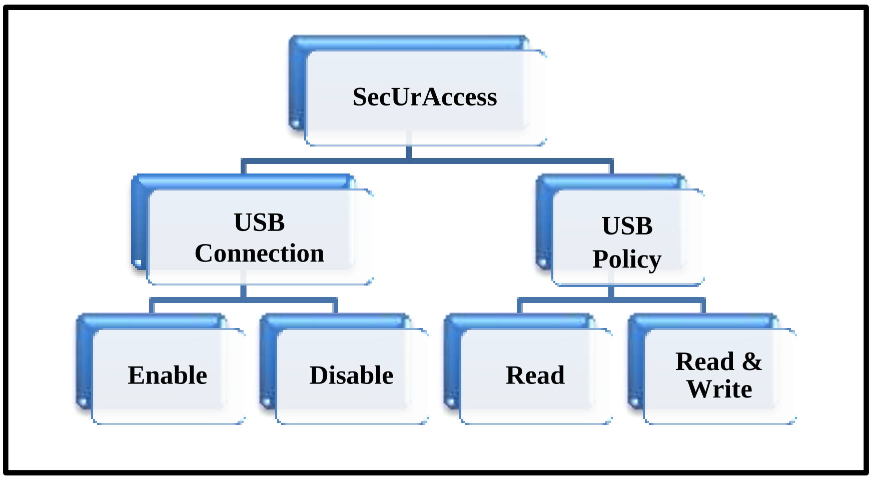


**Figure 1** Overall system design in *SecUrAccess* Software

## 3. System Development

Development and design of the software were built based on the specification that has been formulated according to the function. Figure 2 shows the flowchart of *SecUrAccess* software. Figure 3 shows the screenshot of the design and steps to install and use the *SecUrAccess* software. Table 1 shows the status of USB connection and access rights with description. There are two types of access rights; (i) read-only and (ii) read and write.

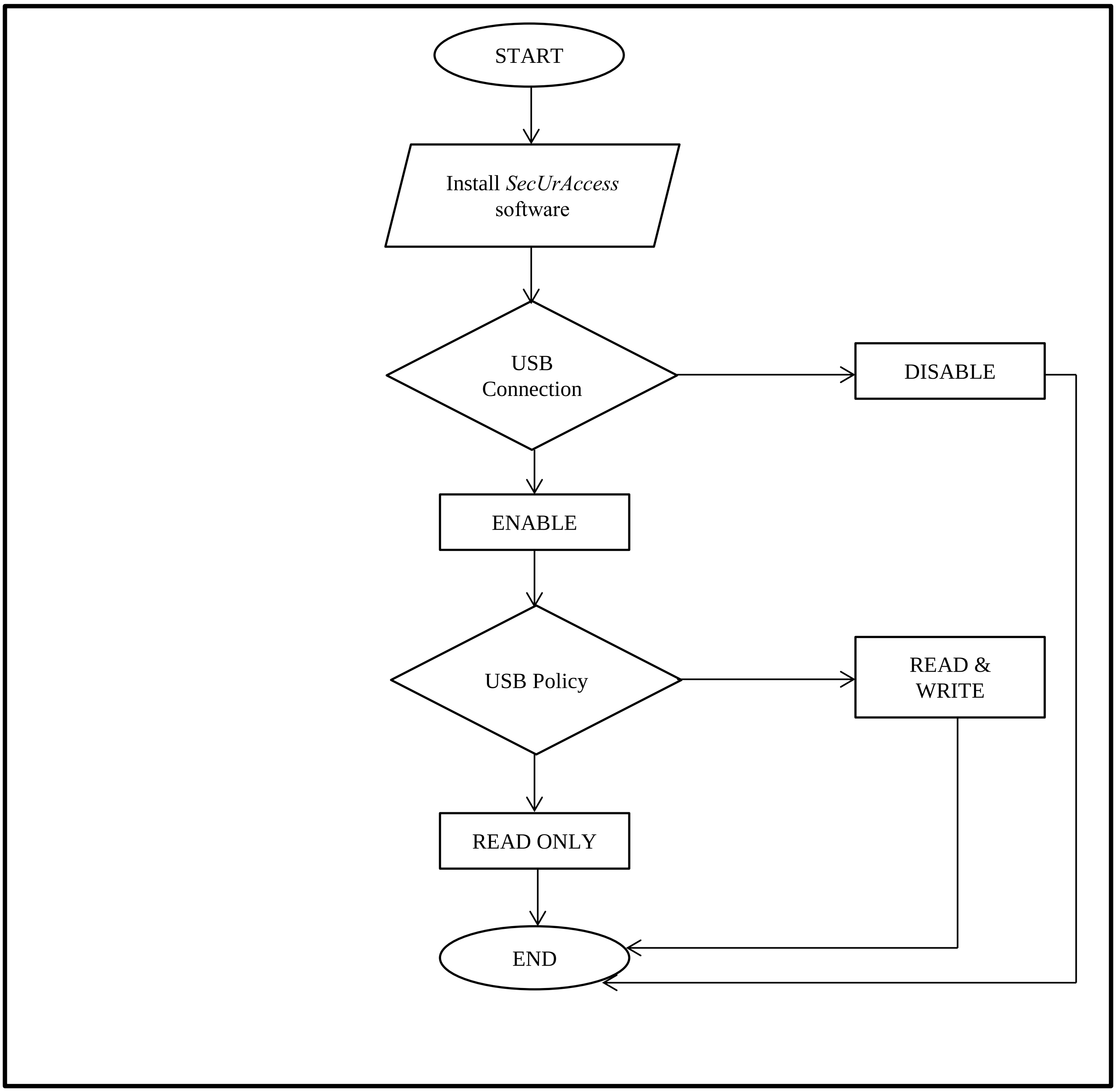
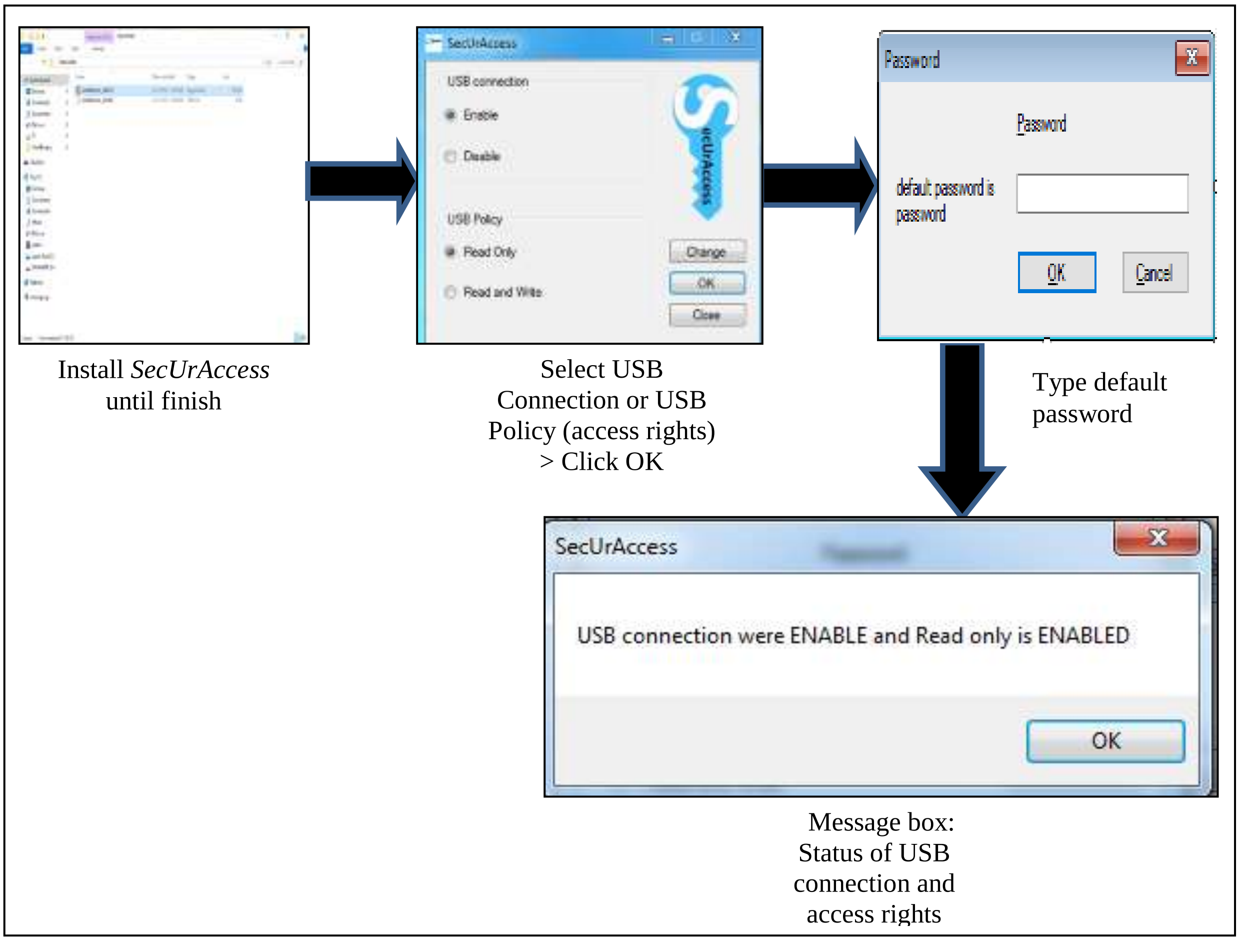


**Figure 2** Flowchart of *SecUrAccess* Software



USB connection
● Enable
○ Disable

USB Policy
● Read Only
○ Read and Write

Password
default password is password

USB connection were ENABLE and Read only is ENABLED

Install *SecUrAccess* until finish

Select USB Connection or USB Policy (access rights) > Click OK

Type default password

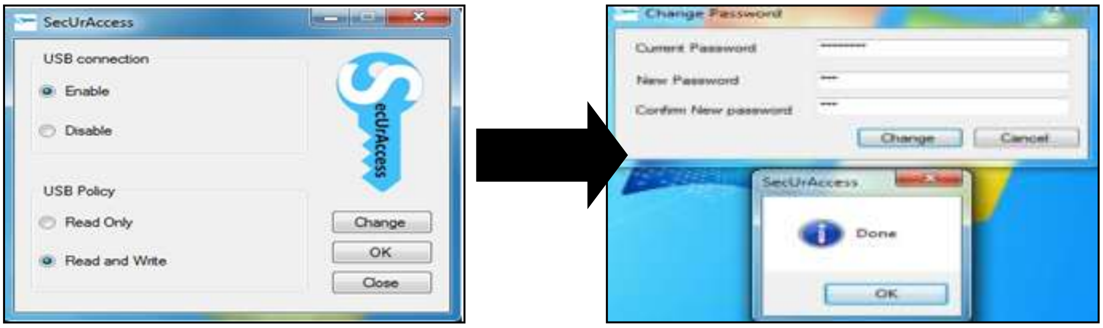
Message box: Status of USB connection and access rights

**Figure 3** Screen Shot of the Design and Steps for *SecUrAccess* Software

**Table 1** Description of USB Connection and Access Rights

| **USB Connection** | **Access Rights** | **Description** |
|---|---|---|
| Enable | Read Only | The user can plug in their USB flash drive but they cannot copy anything from the computer. |
| | Read and Write | The user can plug in their USB flash drive to copy anything from the computer. |
| Disable | - | Windows will no longer start the USB flash drive when detected. |

Figure 4 shows the screen shot of the design and steps for changing password in *SecUrAccess* software.



SecUrAccess

USB connection

● Enable

○ Disable

USB Policy

○ Read Only

● Read and Write

Change Password

Current Password: **********

New Password: ****

Confirm New password: ****

SecUrAccess

Done

Change password interface

**Figure 4** Change Password

## 4. Result and Discussion

The main aim of the system testing is to ensure that the system performs according to its requirement. Testing was conducted by installing the software in several users personal computer to ensure that the software developed is not experiencing any problems. The implementation and testing phase is conducted to demonstrate the software to the users. The software is tested properly in order to provide the benefits for the users as stated by Sommerville (2011). The testing phase also conducted to detect the problems that might occur in the software and the problems that need to be solved immediately to achieve the project objectives. User acceptance testing is a testing that was conducted to test the suitability of the function at the final stage before the software is fully completed. The software was tested on the designated computers and laptop users. The feedback questionnaire was given to the users to share their feedback about *SecUrAccess* software.

### 4.1 Analysis of Testing

Implementation and testing phase is carried out to ensure that the software can achieve the project objectives. The goal of unit testing is to isolate each component of SecUrAccess software and show that the performance of these individual components is correct. Based on this approach, the expected quality of the unit can be tested properly in order to provide benefits to the user (Kamsties et. al., 2013). Unit testing is done to ensure that each individual unit that makes up the software under test is able to function according to the specification. In this phase usually, software defects are typically fixed as soon as they are found, without formally recording incidents. Table 2 shows the testing plan that was conducted.

**Table 2** Test Cases

| Test case ID | Test case description | Expected condition | Actual condition | Result |
|---|---|---|---|---|
| 1 | USB connection ENABLE | When users click ENABLE connection, the user can choose the USB policy. | When users click ENABLE connection, the user can choose the USB policy. | Pass |
| 2 | USB connection DISABLE | When users click DISABLE connection, the user cannot choose the USB policy. The USB policy is not active for the user to choose. The USB flash drive is not detected in USB port of computer or laptop. | When users click DISABLE connection, the user cannot choose the USB policy. The USB policy is not active for the user to choose. The USB flash drive is not detected in USB port of computer or laptop. | Pass |
| 3 | USB policy – Read Only | When user click USB policy - READ Only, USB flash drive can be used to Read Only. The user cannot copy any files or folder to USB flash drive. | When user click USB policy – READ Only, USB flash drive can be used to Read Only. The user cannot copy any files or folder to USB flash drive. | Pass |

| | | | | |
|---|---|---|---|---|
| 4 | USB policy – Read and Write | When users click USB policy – Read and Write, USB flash drive can be used to Read and Write. The user can copy any files or folder to USB flash drive. | When users click USB policy – Read and Write, USB flash drive can be used to Read and Write. The user can copy any files or folder to USB flash drive. | Pass |
| 5 | Change password | The user can change the default password for security purpose. | The user can change the default password for security purpose. | Pass |
| 6 | Log off the computer or laptop automatically after 3 times password attempt failure | The computer or laptop will log off automatically after 3 times password attempt failure. | The computer or laptop will log off automatically after 3 times password attempt failure. | Pass |

The operation phase is where SecUrAccess software is tested. The feedback questionnaire was conducted using Google form and the address link is http://bit.ly/SecUrAccess_Software. Likert scale was used for the respondents to give their feedback. Table 3 shows Likert Scale table. The response from the feedback questionnaire is used to enhance the software to a better version before it is released. Maintenance is done to deliver these changes in the customer environment. Table 4 shows the feedback for item 1-5, 8 and 10 from 20 respondents.

**Table 3** Likert Scale

| | | | | |
|---|---|---|---|---|
| 1 | Strongly Disagree | | Strongly Dissatisfied | Item number 6 (i –v) |
| 2 | Disagree | Item number 1-5, 8 and 10 | Dissatisfied | |
| 3 | Agree | | Satisfied | |
| 4 | Strongly Agree | | Strongly Satisfied | |

**Table 4** Feedback for Item 1-5, 8 and 10

| **#** | **Item** | **Number of Respondent / Percentage** | | | |
|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** |
| 1 | *SecUrAccess* software can protect my data on my laptop / computer from being copied by others using the removable drive. | 1<br>(5%) | 0<br>(0%) | 7<br>(35%) | 12<br>(60%) |
| 2 | *SecUrAccess* software gives privilege for me to enable or disable the USB port from being used to plug in the removable drive (need to restart after the settings). | (5%) | 0<br>(0%) | 10<br>(50%) | 9<br>(45%) |
| 3 | Computer / laptop will switch to log off mode if i enter the wrong password three times in *SecUrAccess* software. | 0<br>(0%) | 3<br>(15%) | 6<br>(30%) | 11<br>(55%) |
| 4 | *SecUrAccess* software runs from a removable storage device, such as a USB flash drive. | 0<br>(0%) | 0<br>(0%) | 11<br>(55%) | 9<br>(45%) |
| 5 | *SecUrAccess* software does not need to be installed on a computer to run and does not store data on the host system. | 1<br>(5%) | 0<br>(0%) | 7<br>(35%) | 12<br>(60%) |
| 8 | I will recommend SecUrAccess software to my friends. | 1<br>(5%) | 1<br>(5%) | 8<br>(40%) | 10<br>(50%) |
| 10 | *SecUrAccess* software has the potential to be marketable. | 1<br>(5%) | 1<br>(5%) | 7<br>(35%) | 11<br>(55%) |

The responses show that most of the respondents agree on the effectiveness of *SecUrAccess* software especially for item number 1 (60%), item number 3 (55%), item number 5 (60%) and item number 10 (55%) which is above 50%. The respondent found that *SecUrAccess* software can be marketable. Where else Table 5 shows the satisfaction rate given for *SecUrAccess* software on its design, quality, performance and user-friendly. Figure 5 shows these results in a graphical format.

● Strongly Disagree
● Disagree
● Agree
● Strongly Agree

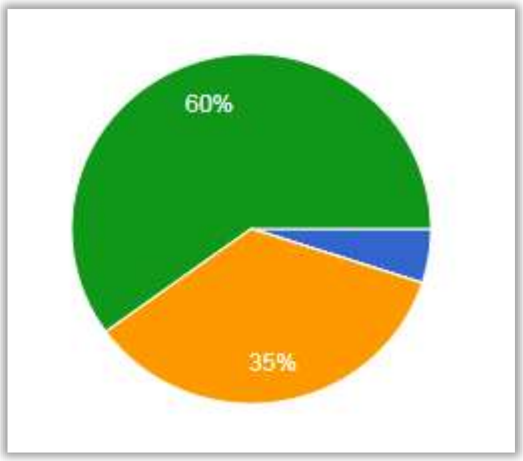


Figure 5a: Percentage for Item 1

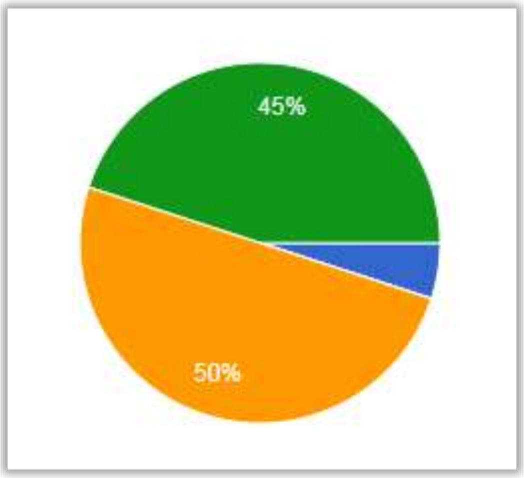


Figure 5b: Percentage for Item 2

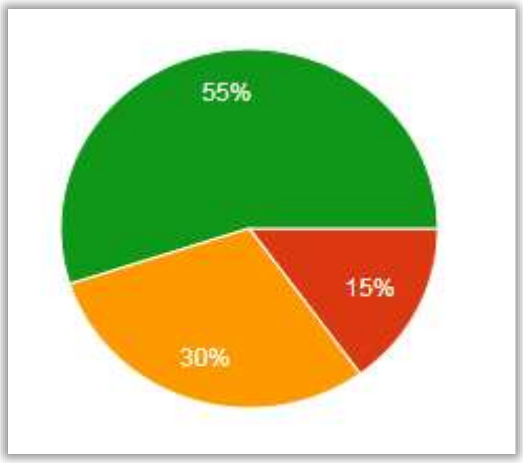


Figure 5c: Percentage for Item 3

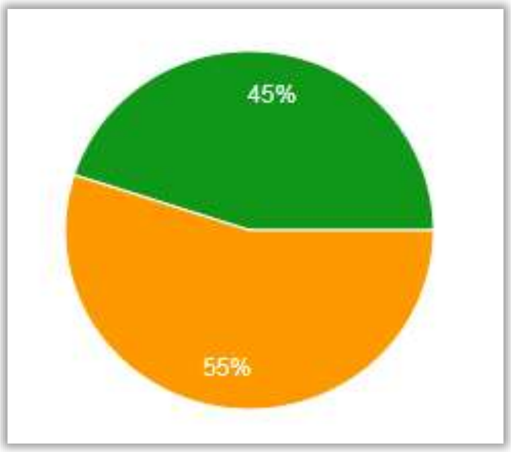


Figure 5d: Percentage for Item 4

cont…

…cont

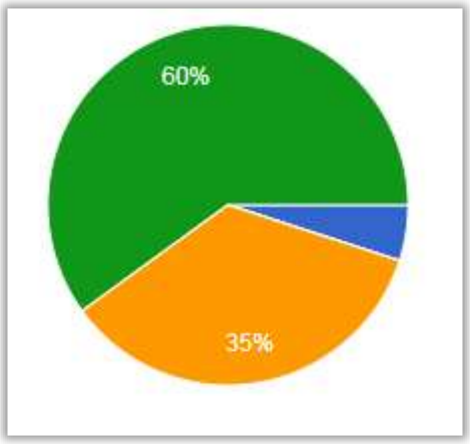


Figure 5e: Percentage for Item 5

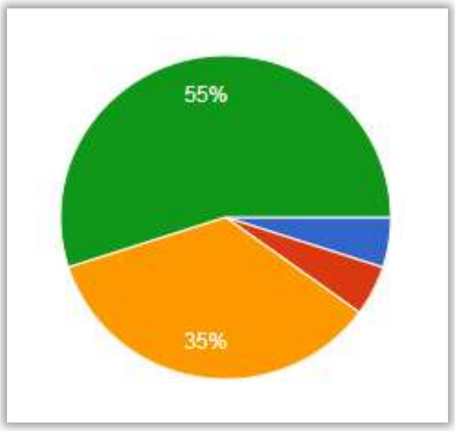


Figure 5f: Percentage for Item 8

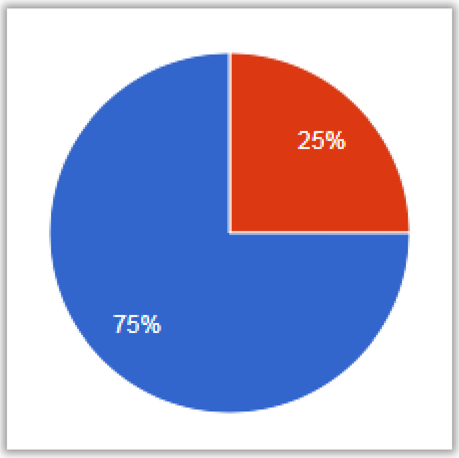


Figure 5g: Percentage for Item 10

**Figure 5** Graphical representation of the analysis results for item 1-5, 8 and 10

**Table 5** Rate of Satisfaction for *SecUrAccess* Software

| # | Item 6 | Number of Respondent / Percentage (%) | | | |
|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** |
| i) | Design | 0<br>(0%) | 0<br>(0%) | 12<br>(60%) | 8<br>(40%) |
| ii) | Quality | 1<br>(5%) | 0<br>(0%) | 8<br>(40%) | 11<br>(55%) |
| iii) | Performance | 1<br>(5%) | 0<br>(0%) | 9<br>(45%) | 10<br>(50%) |
| iv) | User Friendly | 1<br>(5%) | 0<br>(0%) | 9<br>(45%) | 10<br>(50%) |

The highest rate of satisfaction is the total of Satisfied and Strongly Satisfied was given for the design (100%) followed by quality, performance and user-friendly (95%) as shown in Table 5. Overall, the results obtained in the testing of the *SecUrAccess* are satisfactory and the system meets the requirements of the user. Figure 6 shows these results in a graphical format.

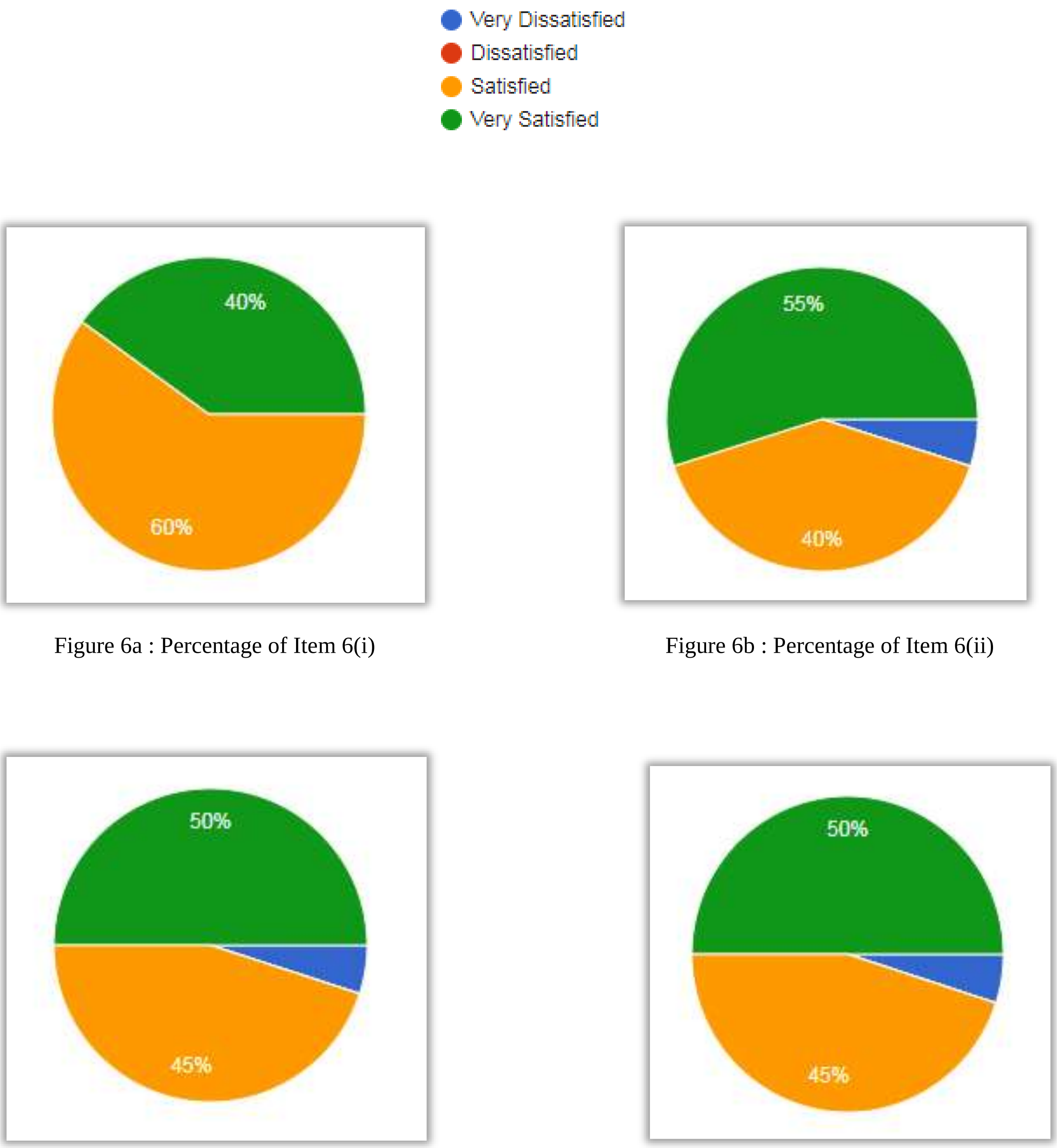


Figure 6a : Percentage of Item 6(i)

Figure 6b : Percentage of Item 6(ii)

Figure 6a : Percentage of Item 6(iii)

Figure 6a : Percentage of Item 6(iv)

**Figure 6** Rate of Satisfaction for SecUrAccess Software

## 5. Conclusion And Future Work

The main purpose to develop *SecUrAccess* software is to provide a gateway in order to protect data in user's computer or laptop from being copied by the unauthorized user. This software can be used in a small, medium or large organization in order to protect valuable information. This software is easy to install and it is user-friendly. Throughout the development of the application, there are some advantages as well as disadvantages that can be identified in the system. Each advantage and disadvantages that are identified during the implementation phase will be referenced in the development of the software in the future. For future studies, it is recommended to work on with log file to identify the USB flash drives that have been plug in the computer or laptop so that the user can identify that someone has tried to get information from their computer or laptop.

Besides that, ongoing organizational awareness, education and training programmes should be conducted to their users to ensure that the use of USB flash drives is properly managed and that the data effectively protected and then removed before their disposal. The personal user also needs education and awareness of the potential dangers that may occur when they dispose the USB flash drives and the measures that can be taken to effectively remove the data and avoid potential data loss.

## References

Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55.

Cooper, P. K. (2017). Organizational security threats related to portable data storage devices: Qualitative Exploratory Inquiry (Doctoral dissertation, University of Phoenix).

Darin, D. (2015). Disable USB Port To Prevent Copying Of Your Database
http://mitchell1.com/knowledgebase/article.php?id=53 [23 June 2017]

Kamsties, E., Pohl, K., Reis, S., Reuys, A. (2013). Testing variabilities in use case models. *Proceedings of the Fifth Workshop on Product Family Engineering, Siena, Italy.*

Silowash, G., & King, C. (2013). Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources. http://repository.cmu.edu/sei/708/ [20 May 2017].

Sommerville, I. (2011). *Software Engineering. 9th edition.* United States: Pearson Education, Inc.

Widya, Chaerani, Nathan, Clarke, C. B. (2011). Information leakage through second hand USB flash drives within the United Kingdom. *Proceedings of the 9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.*