Applied Information Technology And Computer Science Vol. 2 No. 2 (2021) 101-114
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

The Development of Stolen USB Storage with Deduced Location Alert

Loy Mei Ting, Nurul Azma Abdullah[1]*.

Faculty of Computer Science and Information Technology,
University Tun Hussein Onn Malaysia (UTHM),
Parit Raja, 86400, MALAYSIA.

DOI: https://doi.org/10.30880/aitcs.2021.02.02.007
Received 15 June 2021; Accepted 09 September 2021; Available online 30 November 2021

Abstract: Since its invention from the early 2000, Universal Serial Bus (USB) data storage devices including flash drives and external hard disks have become the favorite data storage media devices for students, working professionals, academicians and independent tech consultants. To protect the data in the data storage device from being disclosed, this USB storage device with location alert functionality secure tool is developed. This tool could automatically lock access to the device after certain conditions. Besides that, a user sign-in module is implemented to make it compulsory for user to enter the correct password before accessing to the data storage device. Moreover, user can track the info and approximated geolocation of the device's latest connected computer through email alerts if that computer is connected to internet. Object oriented methodology is used as the methodology to develop this tool and Simple Mail Transfer Protocol (SMTP) was applied to enable automatic email alerts. With this tool, users are able to password protect their USB devices and receive email alerts for the details and approximate location of the devices' latest connected computer. Development of this tool contributes to the protection of USB data storage device by solving issues in which lost or stolen USB device can be easily access by anyone obtained it since it lack of user access control module. Besides that this tool is developed to assist data storage device owner to recover their missing device by sending notification about the device's latest connected computer to the owner.

Keywords: USB data storage device, Password-protection, Email alerts

1. Introduction

USB based memory devices like flash drives and external hard disks are popular because of its high portability, conveniences, cheap price, fast speeds and large capacities. However due to their small size, it can get missing or stolen easily. Losing their USB storage device caused the owners to suffer from serious consequences because the data stored inside the lost or stolen device are facing risks of being unauthorized disclosure, alteration and deletion. There are many circumstances which lead to a missing device - whether it is forgetfully left plugged-in on the public library's computer, accidentally dropped it somewhere or even because forgotten to take it out from our clothes pocket before putting them in the laundry. While most of the cases where USB storage devices went missing is because their owner

* *Corresponding author: azma@uthm.edu.my*
2021 UTHM Publisher. All rights reserved.

forgot which computer it had been plugged to. Moreover, if a USB data storage device went lost or stolen, there is no way to track the location of the device and it is very unlikely to be able to retrieve it back. Hence the owners would suffer serious consequences including losing important data and wasted progresses on the tasks they had been working on the data storage devices. In fact by referring to an article from Kingston Technology, 12,000 customer records lost on average per organization due to missing USB drives [1].

Besides from resulting financial loss and waste of efforts for organizations, missing or stolen USB data storage device also lead to disclose of private data. Owner's personal data such as files and folders might be exploited and duplicated by unauthorised individual. Owners' valuable and private details can be used by malicious party to conduct cyber-attacks toward the owner [2]. USB data storage device's owners must look into this matter seriously since there are lots of news in the newspaper or media publishes about cases of blackmail, extortion, scam and even harassment from the malicious person who extracted the victim's personal information including contact details from their lost devices [2], [3].

Therefore, there is a need to provide assurance for the device's owner by protecting the data in the device from being disclosed by automatically lock access to the device after certain conditions. Be it after some fixed time interval that the data storage device is left idle or upon owner's command. Besides that, it also features a user sign-in module in which entering a correct password is necessary to access to the data storage device. Moreover, owner can track the estimated location of the data storage device's latest connected computer through a user alert functionality if the computer is connected to internet.

The aim of this project is to develop a USB data storage device secure tool with user alert feature. In order to achieve the aim above, few objectives have been set in which:

- To design an USB data storage device secure tool with location alert functionality.
- To develop an USB data storage device secure tool with location alert functionality.
- To perform alpha and beta testing for the functionality of the developed tool.

2. Related Work

2.1 Security Analysis of USB Data Storage Device

Mobile devices like USB data storage devices are easy to succumb to attack against physical security because of their portability and vulnerabilities against unauthorized access. The ways that attackers get the data they want are not limited to theft of the mobile devices as mentioned above. An attacker could also download sensitive data if an unsuspected user were to connect an external hard drive or flash drive to an unsecured computer. Accidentally leaving or losing a USB flash drive on any location outside of an organization is another way for attacker to steal data without ever gaining physical access. Moreover, the malicious payload purposely installed on a USB device would infects an individual computer and possibly the entire network once an unsuspected employee picks up the USB device and inserts it into their computer. An example for this type of attack was an incident happened at a U.S. Department of Defense base in the Middle East in 2008. An employee working at the base inserted a compromised USB memory stick into the government's laptop which resulted in a virus spread undetected throughout the base's systems and sent data back to remote servers in other countries [4].

2.2 Location Tracking Method

To locate a USB data storage device from its connected computer's IP address, utilizing Indoor Positioning System (IPS) would yield better performance compared to Global Positioning System (GPS) as the satellite technologies lack precision when tracking target inside a building. Various

different types of techniques and devices could provide indoor positioning and the major methods included Wi-Fi-based positioning system (WPS) and Bluetooth technology [5].

WPS is a geolocation system that discovers and locates a device location by utilizing nearby Wi-Fi hotspots and wireless access points. The basic localization technique used for wireless access point positioning is based on measuring the intensity of received signal strength indication (RSSI). RSSI localization method works by measuring signal strength from the client device to different access points and determine the distance between client device and access points by combining those captured information with a propagation model. Although RSSI localization is one of the easiest and cheapest methods, it having a major disadvantage where it could not locate device with high accuracy as the RSSI measurements prone to be unstable due to changes in physical environment or multipath fading [6].

Bluetooth access points of network can be used for location tracking. Device's physical location proximity is deduced by analyzing signal strength received from access points. However, Bluetooth was not intended to provide precise location tracking like GPS, it is more concerned about the proximity of device but not about the device's exact location.

2.3 Alerts Sending Method

Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission. It is a connection oriented and text-based protocol in which the E-mail sender are required to issue command strings and supplying necessary data over a Transmission Control Protocol (TCP) connection in order to communicate with the E-mail recipient. An open SMTP session consists of commands from SMTP client and corresponding responses from SMTP server to exchange session parameters. To send an E-mail, SMTP transactions require three parameters to initiate a command/reply sequences:

i. Mail command: To establish return address, so automated message from E-mail system could notify sender that about the E-mail delivery status.

ii. Recipient (RCPT) command: To establish recipient of message, the mail transfer agent uses DNS to identify and connects to the recipient's E-mail domain server so mail exchange could be completed.

iii. DATA: To signal the beginning of E-mail's text message and the content of message.

2.4 Reviews on Existing Tools

This section will review two existing secure tools for USB data storage device which are Lock USB and GadgetTrak. Each of their respective features, advantages and disadvantages will be explained below and this section will be concluded with the comparison between existing tools with the proposed tool.

2.4.1 Lock USB

Lock USB is a USB password protection and security tool developed by Lock USB Inc., an United States of America company in year 2016. Among the features provided by this software included cross-platform protection, it is able to prevent access to locked data in other operating systems including Windows, Mac, Linux, and FreeBSD. Besides that, this software supports a wide range of file system. It is fully compatible with FAT32, NTFS and FATex file systems and ensures compatibility for all external drives too. Moreover, Lock USB offer plug and play protection where it takes only a few seconds to setup and lock the entire drive. The advantages of Lock USB are the software has a small size in which the installer merely took 120kb. Secondly, the lock and unlock process is quick where users are able to lock or access their data within seconds. Thirdly, it works with any type of external drive such as compact flash cards, USB thumb drives and external hard drives. However it has some

disadvantages too such as it could not lock automatically and the users must lock the device manually. Besides that, it does not offer a solution for users to search and retrieve their lost devices back.

2.4.2 GadgetTrak

GadgetTrak is a theft recovery and location tracking software developed by an American company under the same name in year 2007. It is claimed to be the first theft recovery product for USB mass storage devices including iPods, flash drives, digital cameras and other devices when connected to a computer [7]. The advantages of GadgetTrak included that the software featured an online dashboard which allow users to track multiple laptops and smartphones at once. Besides that, the software is able to generate and fill an online police theft report with the location tracking details. However it has some disadvantages too such as the software does not have data protection or backup functionalities. Secondly, the software is not stealth and can be removed by the thief if the Administrator account isn't properly protected.

2.4.3 Comparison between Existing Software with the Proposed Tool

For existing USB devices protection software, two existing software had been reviewed in the previous sections. The first being Lock USB, a USB devices password protection and security tool while the second is GadgetTrak which is a theft recovery and location tracking software. In this section, these two existing software are compared together with the proposed tool. Table 2.1 is the comparative analysis of the three software.

Table 1: Comparative analysis of different tool

Features	Lock USB	GadgetTrak	Proposed Tool
Cross platform	YES	NO	YES
Password protection	YES	NO	YES
Lock automatically	NO	NO	YES
Master key	YES	NO	YES
Location deduced from IP address	NO	YES	YES
Alert functionality	NO	YES	YES

Table 1 shows the comparative analysis of different tool. The tools are Lock USB, GadgetTrak and the proposed tool. The proposed tool aims to implement the perks from both existing software, therefore the planned features for the proposed tool included cross-platform support, password protection, automatic lock function, master key support, deduced location tracking and user alert functionality.

3. Methodology

The selected methodology models for the development of this project is object oriented analysis and design (OOAD) methodology model. Object oriented methodology is a project development approach which facilitates the re-use of software components. By adapting to this methodology, a program can be developed on component basis where the sharing and re-use of existing components by other systems is enabled. Hence a software development process with higher productivity and lower maintenance could be achieved by adopting object oriented based methodology model[8]. OOAD can be divided into two main categories where the first being object oriented analysis (OOA) which focus on investigation of objects while the second being object oriented design (OOD) which is relationships of identified objects. The OOAD methodology model is broken up into different stages during the software development life cycle. These stages included object oriented analysis requirement, object oriented design, object oriented implementation, object oriented testing and object oriented deployment [8].

3.1 Requirement Gathering and Analysis Phase

Object oriented requirement analysis phase is the planning phase where a clear picture of the pr0oposed system is formed. First an issue is identified from daily life observations. It is identified that the uses of USB data storage device pose information security threats. The discovered issue are looked into details and analyzed. Three problems had been defined at this point where the first being USB devices can be easily stolen or went missing due to its small size and portability. Secondly it lacks of access control feature where the USB device can be access by anyone who obtained it. Third, it lacks of user alert system to notify users about the device's current location.

Requirement analysis is the process of defining, documenting and maintaining requirements. In this process, functional and non-functional requirements of the tool are identified and analyzed. Sections below discuss about each respective requirements in details [9]. Functional requirements define the basic behavior of the program and how the program responds to inputs. Functional requirement are also the features which allow program to function as intended, a program will not work if functional requirements are not met [9]. Table 2 shows the functional requirements of the proposed tool.

Table 2: Functional requirement for the tool

Module	Functionalities
Register user	Register user's information to bind the USB data storage device System alert for any invalid input
Login	User inputs valid password System alert for any invalid input
Device locker	Lock access to the device after the device remains idle for fixed time or upon owner's command Require owner enter password to unlock
Location tracker	Extract device details from the computer which are plugged with the USB data storage device Required that the computer is connected with internet to allow Wi-Fi positioning.
User alert	Send alert to owner with the details of connected computer, required internet connection on the connected computer to work.

From the table above, five modules featured in the tool and each of their respective functionalities is being discussed. This tool concentrates on automatically lock access to the data storage device after a fixed time interval or upon owner's command. Besides that, a user access control module is also included to allow authorized user to unlock and access the data storage device.

Non-functional requirements are criteria that can be used to judge the operation of a program. Non-functional requirements are normally known as the quality attributes of a program and they also define the behavior, features, and general characteristics which will affect user experience [10].

Table 3: Non-functional requirement for the tool

Requirement	Description
Performance of user interface and system flow	Correct tool's interface should be display and the system run without error
Operational	Part of the tool's functionality is only available when internet connection are available

Table 3: (cont.)

Requirement	Description
Security	User may access the system with correct username and password Password is encrypted Password must be combination of upper and lower case alphabets, numbers and special symbols to meet requirement of strong password management

Table 3 shows three non-functional requirements of the proposed tool had been identified. The proposed tool aimed to provide smooth and error-free experience for the users. Secondly, part of the functionalities of the tool is only available when internet connections are available for the host computer. Third, to achieve security non-functional requirement, users should set their password with combination of upper and lower case alphabets, numbers and special symbols to meet requirement of strong password management.

After the problems are defined, the objectives and the scopes of the proposed tool had been identified. There are three objectives in this project which is to design, to develop and to test the proposed tool. For software and hardware requirement of the proposed tool, Table 4 has shown the requirement of software and hardware to develop this tool.

Table 4: Software and hardware requirement

Requirement	Specification/Description
Hardware requirement	i. Computer: • Minimum of 1Gb hard disk space • Minimum of 2Gb RAM • Intel Core i7 Processors ii. USB flash drive: • Minimum 2Gb of disk space
Software requirement	i. Microsoft Windows 10 Operating System ii. PyCharm Community Edition IDE iii. ImDisk Virtual Disk Driver
Programming Language	i. Python

Table 4 shows the requirement of software and hardware used in this project. The computer use should have the minimum hard disk space of 1Gb and 2Gb of RAM which is mainly use for development of the tool and report writing. Next, USB flash drive is required to test and run the developed tool. PyCharm Community Edition is the IDE that is used to build built the tool and Python programming language is used to build the tool. An open-source software ImDisk Virtual Disk Driver is used to create RAM drive in the USB flash drive.

3.2 Object-oriented Design Phase

In this phase, the complete architecture for the proposed tool is designed. For this tool six classes are designed and link together using object-oriented programming method. The six classes design are “User”, “Installation_Update”, “Login”, “Email_Alert”, “Tracker” and “Device_Lock”.

Lastly is the user interface design, user interface design is to make sure that users are able to use the tool without trouble. There are five user interface designs in this phase. Besides that, test plans are designed for the developer to measure if the end product meets its design specifications and other

requirements. User acceptance form is also important as it allow users to evaluate the test cases of the end product.

3.3 Object-oriented Implementation and Testing

In implementation phase, the design of classes and user interface are implemented. All classes and user interfaces are link together to make sure that the tool function well as user interface is important to allow user access the tool with ease. In testing phase, the designed test plan is used to ensure the proposed tool is functional as expected. If any error happens, the debugging process is take place to ensure that the tool is functioning. For testing, a test plan is used to test the functionalities of the proposed tool. The test plan is divided into four main categories which included user interface testing, system functionality testing, security requirement testing and input validation testing. Object oriented testing is carried out to ensure the functionality of the tool will adhere to the objectives and requirements of the project.

3.4 Object-oriented Deployment

In object-oriented deployment stage, the development process is carrying out by adhering to object-oriented programming method. Among the object oriented concepts to be applied included encapsulation, inheritance and polymorphism. Besides that, there are three important steps involved to write a program. The first step is declaring class to establish the object's data and functions. Secondly is instantiating class to establish object. The third step is to invoke message to establish object communications.

3.5 Object-oriented Maintenance

Software maintenance is the last phase of software life cycle. It is aimed to maintain the software system to keep up with the advancement in software and hardware technology so that the lifecycle of the software can be prolonged [11]. Among the common problems faced by developers when maintaining an object-oriented system included software understanding problems and the complex dependencies in object-oriented classes' problems. Therefore maintainer need to spend a lot of time and resources in order to understand the object-oriented software system process by reading a class relationships, inherence, polymorphism, tracing and manually comparing the source code in the object-oriented software system [12].

4. Result and Discussion

4.1 Modules of the proposed tool

This tool focuses on applying relevant information security knowledge and technique to analyse and extract details from the computer connected with the data storage device so that the owner is able to track down their device. A RAM disk is created and act as a secret storage in the USB data storage device where the RAM disk could only be mount and access after the users login to the tool installed in their USB data storage device. This proposed tool also concentrates on automatically lock access to the data storage device after certain conditions, be it after a fixed time interval or upon owner's command. Besides that, a user access control module is also included to allow authorized user to unlock and access the data storage device. The modules for the tool are shown in Table 5.

Table 5: Modules for the proposed tool

Module	Function
Register owner	Register owner's information to bind the USB data storage device. Information collected included owner's name, contact details, password, security question, and answer for security question.

Table 5: (cont.)

Module	Function
Login	To enable USB data storage device's owner to access their device. Password is encrypted with Fernet symmetric encryption algorithm.
RAM disk creator	A RAM disk that act as a safe and secret storage is created during tool setup and only mount when owner successfully login to the tool.
Device locker	Lock access to the device after the device remains idle for fixed time or upon owner's command. Require owner enter password to unlock.
Tracker	Extract device details from the computer which are plugged with the USB data storage device. If the computer is connected with internet, this module will locate its location via Wi-Fi positioning.
User alert	Send alert to owner with the details of connected computer, required internet connection for the connected computer to work.

4.1 General System Architecture of the Tool

General system architecture is a conceptual model which shows a system's structure, behavior and viewpoint framework [13]. System architecture included the system components and sub-systems developed which will work together to form an overall system. System architecture also defines the system's components and fundamental organization. Besides that, it shows their relationships to each other and to the environment, and the principle governing the system's design too. Figure below shows the system architecture design of the proposed tool.

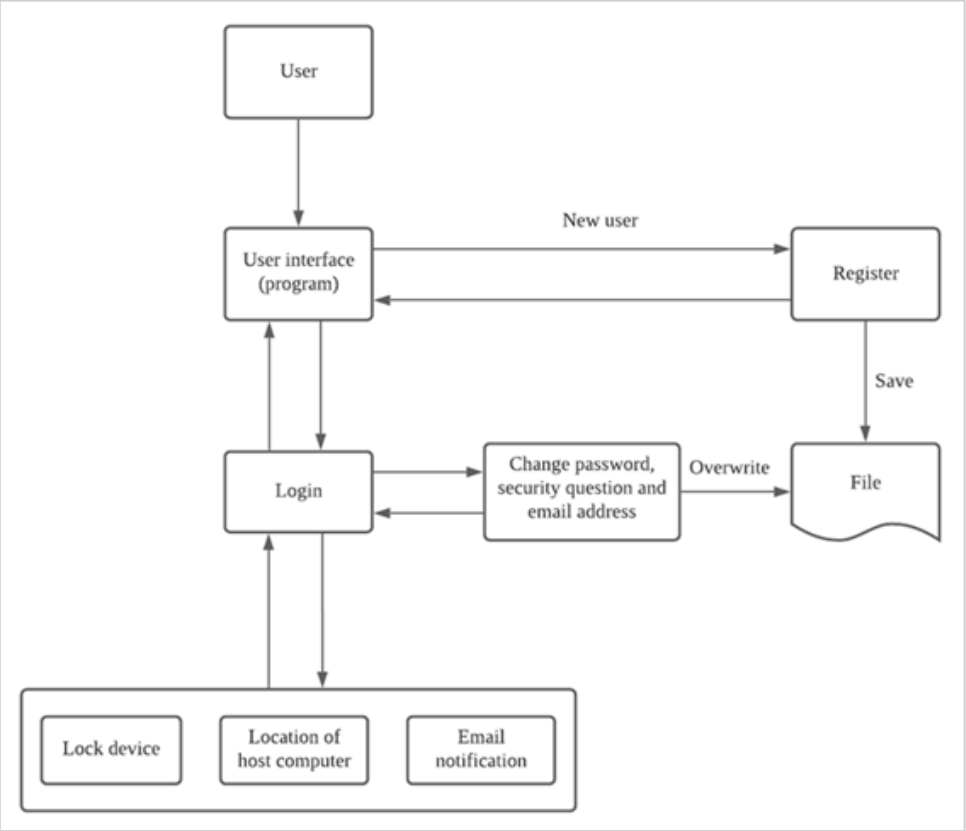

Figure 1: System architecture design of the proposed tool

Figure above shows the proposed tool's system architecture design. First when the users launched the tool, users would need to either register themselves if they are new user or proceed to login in order to unlock their USB device which had been lock previously. After the user authentication process, users

can choose to change their password, security question and its answers and the email address for receiving email alerts. Users can then proceed to manually lock their USB device and logout. The tool will send emails written with the details and location of host computer that is plugged with the USB device after a fixed interval.

4.2 Unified Modelling Language (UML)

UML (Unified Modeling Language) is the standard language for specifying, visualizing, constructing, and documenting the software system [9]. Sections below present use-case diagram, sequence diagram, activity diagram and class diagram of the proposed tool.

4.2.1 Use-Case Diagram

Designing use case diagrams could assist the developer to gather the requirements of a system including internal and external influences. These internal and external agents are known as actors. Use case diagrams consist of actors, use cases and their relationships [14]. However, since all functionalities for this proposed tool is the same and available to all categories of user thus there is only one use-case diagram as show in figure below.

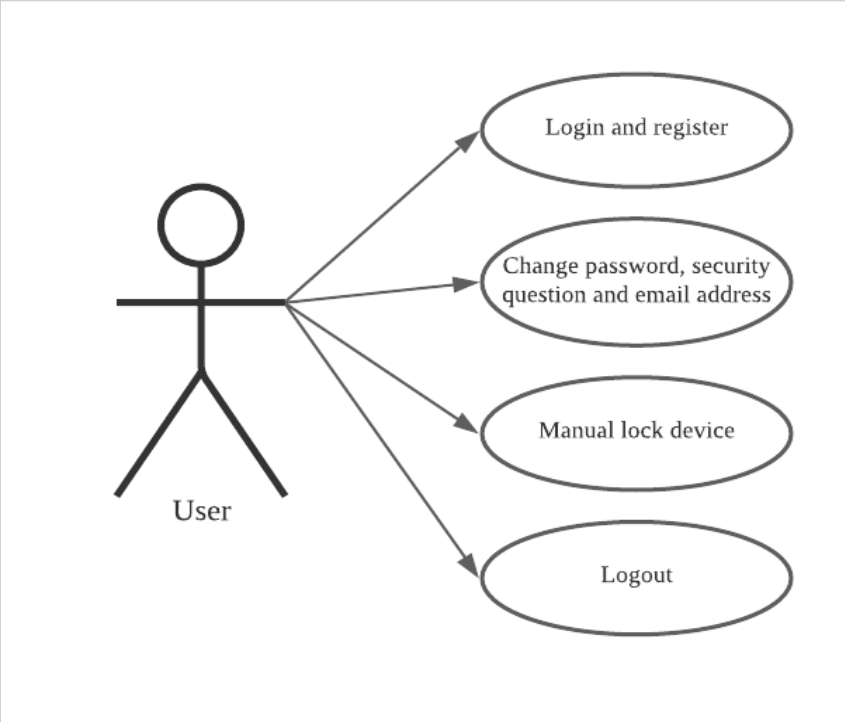

Figure 2: Use case diagram for user

From the figure above, there are four functionalities that can be performs by user. Those functionalities included login and register themselves, configure security settings (change password, change security question and its answer and change email address which receive alerts), lock USB device manually and logout from the tool.

4.2.2 Activity Diagram

Activity diagram is the flowchart to represent the flow of system between activities; activities are the operations running on the system. Activity diagram are able to capture the dynamic behavior of the system. Generally the other UML diagrams are used to show the message flow from one object to another but activity diagram is used to show message flow from one activity to another [15]. Figure below shows the activity diagram for the proposed tool.

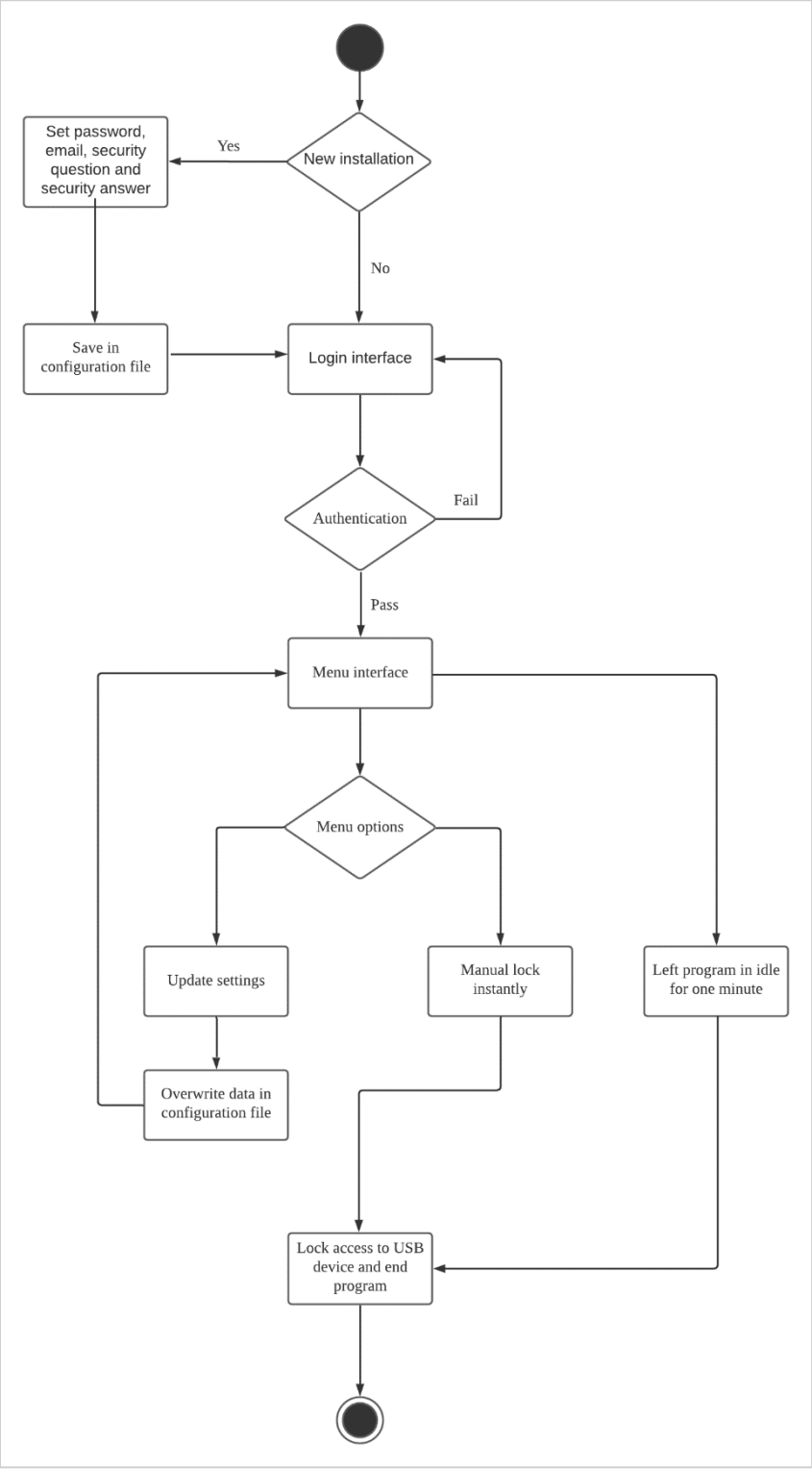

Figure 3: Activity diagram for the proposed tool

Figure above shows the activity diagram for the proposed tool. When the users first launched the tool, they will encounter the login interface. If the tool is being launched in a USB device for the first time, users are required to set a password to lock the USB device, set a security question and its answer and set an email address to receive email notification. If the tool had previously installed on the USB device, users are required to enter their password to unlock the device. After the user authentication process, users will proceed to the user panel where they could choose to either update their security settings or to manually lock their USB device then procced to logout.

4.3 Summary of Testing

For system testing, two methods are used in which the first being functionality testing through test plan and the second is user acceptance testing.

4.3.1 Test Plan Result

System test is applied to the developed system according to the pre-defined test plan in previous chapter. The results of system test are shown in table below.

Table 6: Table of test plan results

Test category	Expected result	Actual result
Installation of tool	• Able to detect if the tool had been previously installed. • Record the user input credentials to configuration file.	Pass
Login	• User able to login after entering correct password. • Display error message when invalid password are inputted. • Prompt out security question after the user failed to input correct password after three consecutive attempts. • Allow user to access if user answered security question correctly. • Login interface switch to menu interface after successful login.	Pass
Update settings	• Interface to update settings appeared. • Display error message when fields are left blank. • Display error message when the user's input breach the input validation standards. • Record the user's input to configuration file.	Pass
Tracker functionality	• Discover host computer's name and details. • Discover host computer's IP address. • Deduce host computer's geological location. • Record the collected information.	Pass
Email sending functionality	• Compose an email with user's email address as recipient. • Input the collected information as email content. • Send the email to user's email.	Pass
Device lock functionality	• Perform USB device lock when user chooses to lock manually at menu interface. • Perform USB device lock after the host computer is left idle for a fixed interval.	Pass

In these different categories of testing and security checklist for the developed tool, all of the requirements pre-defined in the previous chapter are being fulfilled. This indicates that the developed tool is well-functioned and could be proposed for public use.

4.3.2 User acceptance test

The results of the user acceptance form are separate into two categories. The first being the results for system testing and the second category are regarding the security check list for the developed tool. Graph below shows the results for users' system test.

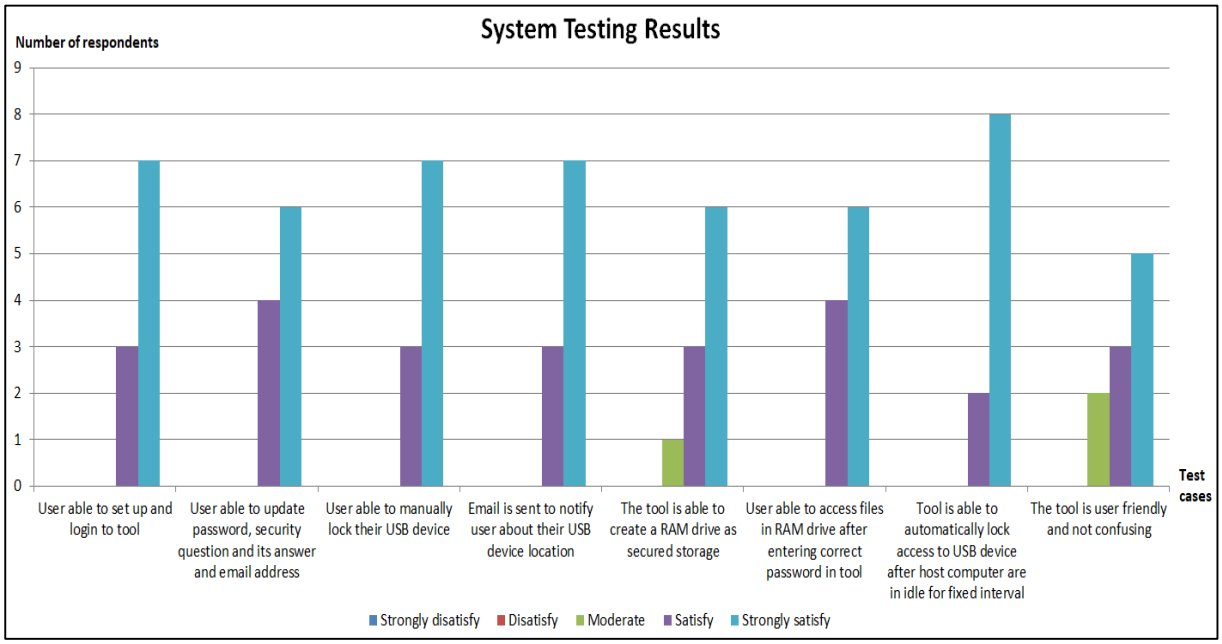

Figure 4: System testing results

Figure above shows the results of the system testing performed by 10 respondents. Seven respondents strongly satisfy that users are able to set up and login to the tool, manually lock their device and received notification email from the tool. Besides that, six respondents strong satisfy about the different functionalities of the tool. Overall, the responses received from all of the respondents ranged between moderate and strongly satisfy. Therefore it can be concluded that all respondents are satisfied with the system functionalities. The results for security checklist test performed by respondents are shows on figure below.

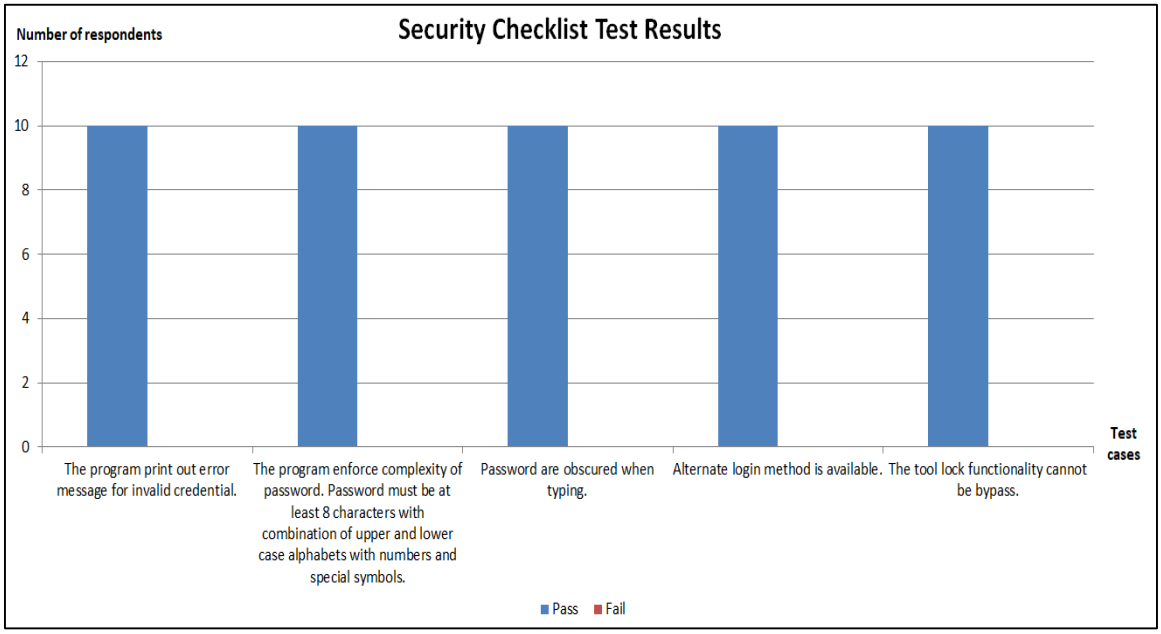

Figure 5: Security checklist test results

Figure above shows the security checklist test results. Five security elements had been check and test by 10 respondents. All security checklist criteria pass the testing with all 10 respondents satisfied with the security elements implemented in the system.

5. Conclusion

The proposed USB storage secure tool has some advantages. The first advantage is that the tool provides back-up login method which the users can login by answering to their pre-defined security question if they forgot their password. Secondly, the developed tool is able to send email alerts to users to notify them their USB devices are currently connected to which computer and the approximated geolocation of the device. Third, the sensitive credentials of users are encrypted using Fernet symmetric encryption algorithm which assures the confidentiality as well as integrity of the credentials. Moreover, instead of partitioning the USB storage disk space, a RAM drive act as user's secured storage is mounted when users successfully login to the tool. The fifth advantage is there is an automatic lock function to unmount the RAM drive and logged user out from the tool if the system remained idle for one minute.

However, the proposed USB storage secure tool has several disadvantages. The disadvantages are the tool is only applicable to Windows operating system. Secondly, the geolocation tracking functionality does not yield high accuracy as it is based on Wi-Fi positioning system which is more concern about proximity and not about exact location. The third disadvantage is the geolocation tracking functionality unable to detect and counter against IP addresses spoofing or the uses of VPN to mask the host computer's IP address, which resulting the tool unable to locate the host computer's true location. And lastly, the credential file stored inside the USB storage device might get corrupted when the USB storage device is booted.

Several recommendations are suggested to be implemented in order to improve the functionality and performance of the developed USB storage secure tool. Recommendations for future work included that the tool shall be able to run cross-platform in different operating systems. Secondly, implementing paid geolocating API services might yield more accurate results and better performances. Third, create graphical user interface (GUI) for greater usability.

Overall, the developed USB storage secure tool has accomplished the requirements and objectives that pre-defined in previous chapters. Users can use the developed tool to secure their USB storage and receive email alerts.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] S.-H. I.-Y. Lee, "A Study on Security Solution for USB Flash Drive," J. Korea Multimed. Soc., vol. 13, no. 1, pp. 93–101, 2010.

[2] D. B. M. Yin, H. Ramadhani, and M. S. M. Salleh, "Smart Lock and Smart Alarm: Alert and protect your lost USB flash drive," in Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, ICUIMC 2014, Siem Reap, Cambodia, 2014, doi: 10.1145/2557977.2558010.

[3] S. H. Lee, K. Bin Yim, and I. Y. Lee, "A secure solution for USB flash drives using FAT file system structure," in Proceedings - 13th International Conference on Network-Based Information Systems, NBiS 2010, Takayama, Gifu, Japan, 2010, pp. 487–492, doi: 10.1109/NBiS.2010.30.

[4] W. J. Lynn III, “Defending a New Domain | Foreign Affairs,” Foreign Affairs, Council on Foreign Relations, 2010.

[5] P. E. Lopez-De-Teruel, F. J. Garcia, O. Canovas, R. Gonzalez, and J. A. Carrasco, “Human behavior monitoring using a passive indoor positioning system: A case study in a SME,” Procedia Computer Science, 2017, vol. 110, pp. 182–189, doi: 10.1016/j.procs.2017.06.076.

[6] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, “SpotFi: Decimeter Level Localization Using WiFi,” ACM SIGCOMM Comput. Commun. Rev., vol. 45, no. 4, pp. 269–282, Sep. 2015, doi: 10.1145/2829988.2787487.

[7] Bertoni Steven, “Most Stolen Electronics,” Forbes News, p. 17, December 23, 2008. [Online]. Available: Forbes News, https://www.forbes.com. [Accessed October 29, 2020].

[8] L. Leimane and O. Nikiforova, “Mapping of Activities for Object-Oriented System Analysis,” Appl. Comput. Syst., vol. 23, no. 1, pp. 5–11, Jun. 2018, doi: 10.2478/acss-2018-0001.

[9] H. Herchi and W. Ben Abdessalem, “From user requirements to UML class diagram,” in International Conference on Computer Related Knowledge, July 5-7, 2012, Sousse, Tunisia, pp. 89–92, doi: 10.1109/ICCRK.2012.51.

[10] H. Wada, J. Suzuki, and K. Oba, “Modeling non-functional aspects in service oriented architecture,” in Proceedings - 2006 IEEE International Conference on Services Computing, SCC 2006, Chicago, Illinois, USA, September 18-22, 2006, pp. 222–229, doi: 10.1109/SCC.2006.74.

[11] M. L. Domsch and S. R. Schach, “Case study in object-oriented maintenance,” in Conference on Software Maintenance, Oxford, England, August 30-September 3, 1999, pp. 346–352, doi: 10.1109/icsm.1999.792632.

[12] H. J. Al-Fawareh, “Modeling an Object Oriented for Maintenance Purposes,” Int. J. Comput. Technol., vol. 3, no. 3, pp. 401–405, Nov. 2012, doi: 10.24297/ijct.v3i3a.2945.

[13] H. Jaakkola and B. Thalheim, “Architecture-driven modelling methodologies,” Frontiers in Artificial Intelligence and Applications, vol. 225, pp. 97–116, 2011, doi: 10.3233/978-1-60750-690-4-97.

[14] B. Dobing and J. Parsons, “How UML is used,” Communications of the ACM, vol. 49, no. 5. Association for Computing Machinery, pp. 109–113, May 2006, doi: 10.1145/1125944.1125949.

[15] H. Chen, J. Jiang, Z. Hong, and L. Lin, “Decomposition of UML activity diagrams,” Softw. Pract. Exp., vol. 48, no. 1, pp. 105–122, Jan. 2018, doi: 10.1002/spe.2519.