OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-27 (Feb. 2020)
5th International Conference On "Innovations in IT and Management"
Organised by: Sinhgad Technical Education Society's
SINHGAD INSTITUTE OF MANAGEMENT AND COMPUTER APPLICATION (SIMCA),
Narhe Technical Campus, Pune, Maharashtra (India) 411041.
Held on 6th & 7th February 2020

Setting Barrier to Removable Drive through Password Protection for Data Security

S. K. Kharade[#1], K. G. Kharade[*2], R. K. Kamat[*3],V. S. Kumbhar[*4]

[#]*Department of Mathematics, Shivaji University*
Kolhapur, India
[1]*shraddha.k.kharade@gmail.com*

[*]*Department of Computer Science*
Shivaji University
Kolhapur, India
[2]*kabirkharade@gmail.com*
[3]*rkk_eln@unishivaji.ac.in*
[4]*vsk_csd@unishivaji.ac.in*

Abstract

In the computational world all kind of communication is now using USB as it is globally recognized hardware standard of communication. Removable devices are very useful portable storage devices which are generally used for transferring computer data from one computer to another. Commonly removable devices are used to store a variety of information, some of which are greatly important. It has become inevitable to secure our computer system from unauthorized individuals which may steal our personal data. This can happen by connecting any external storage device, thus we need to take proper precautions to protect data. With the requirement to guard important data present on the computer systems Removable Device Locker came into reality. It is inimitable type of system which is developed to secure the significant data in the computers. Using this system, user can restrict unauthorized access of removable devices. If the system administrator disables the device manager's universal serial bus controller's settings manually; even novice computer user can enable the above settings and can start accessing target machine. Instead of assembling USB settings manually Removable Device Locker can be used. The main idea of this application is to enable or disable the access of removable device to computer system.

Keywords: *Intruder, Malicious software, Novice user, Text password, Un-authorized user, USB, Virus*

1. Introduction

With the speedy development of information technology, the communication standard has changed a lot. As communication is very important characteristic of every work, means of communication has to be more resourceful and more protected. Since the marketable success of the Removable Device for transferring data, they have become the most common means of transferring data. The main aim behind developing Removable Device was to make it simple to connect to system. The demand for these removable storage devices has been immensely enlarged. With all these elasticity, risks have also come into picture. Removable devices can store and spread malwares also. We use removable storage devices to transfer information or to

keep back-up of data. It can lead to the outflow of information. The outflow of data makes the information insecure. This flexibility of directly accessible of copying any data from the computing device can make the data insecure. It allows the unauthorized users to access the data and copy/erase the data from your computing device and misuse it in any ways. The organizations are at risk when any sensitive information is easily copied with the help of these removable storage devices by the employees and taken out of the workplace and misuse it or being given to any other companies. This show the way to pay huge amount of loss for losing the information that can include important research work, beneficial organization data, confidential data, personal data and many more. As easily we can transfer the files between the removable device and the system at the same point. The viruses can also be transferred from the removable device to your computing devices. These viruses and any malevolent programming can degenerate your information which prompts information misfortune. On the off chance that somebody intentionally needs to modify every one of your information it just wants to stopped the capacity gadget which contains the infections and move it to your processing gadget.

The target machine's USB ports are enabled by default. If you are not using USB devices in a machine you can disable its USB controller settings. When a target machine is in operation, a USB device is plugged into the computer, the device automatically connects to the computer. This auto connect feature can be disabled. It is easily possible for any user to enable or disable this feature. For all these reasons Removable Device Locker application comes into picture to protect from unauthorized access. It is an application having password protection to keep out unauthorized users from your computer system. Anybody can copy your system data or numerous types of viruses can enter your computer through removable devices. Intruders can damage your important files. This application provides interface to enable or disable removable drive access. In order to enable the access user needs to enter Administrative Password.

2. Working Model

From the present problem segment, it is noticed that, existing applications are inadequate to offer security facilities and also they lack in providing well-built access control system. To solve these troubles, we propose to implement our Removable Device Locker application. It primarily provides facilities for locking or unlocking access to computer system through removable devices. For making authentication harder security of text password is used. If they make success over text password then they can connect the removable device to the computer system. Text password is a first verification step in this system. Text password will get validated against the original passwords stored in the database, if they match then only user can have access to the system. If neither of the entered passwords matches, then system will simply shutdown. Client is furnished with three opportunities to enter secret word once more.

Fig. 1. Removable Device Locker application

3. Methodology

Initially Removable Device Application Lock needs to be installed on the computer system. Whenever an external storage device is attached to a computer, application starts running. A window appears on the computer screen with two options: ENABLE-DISABLE.

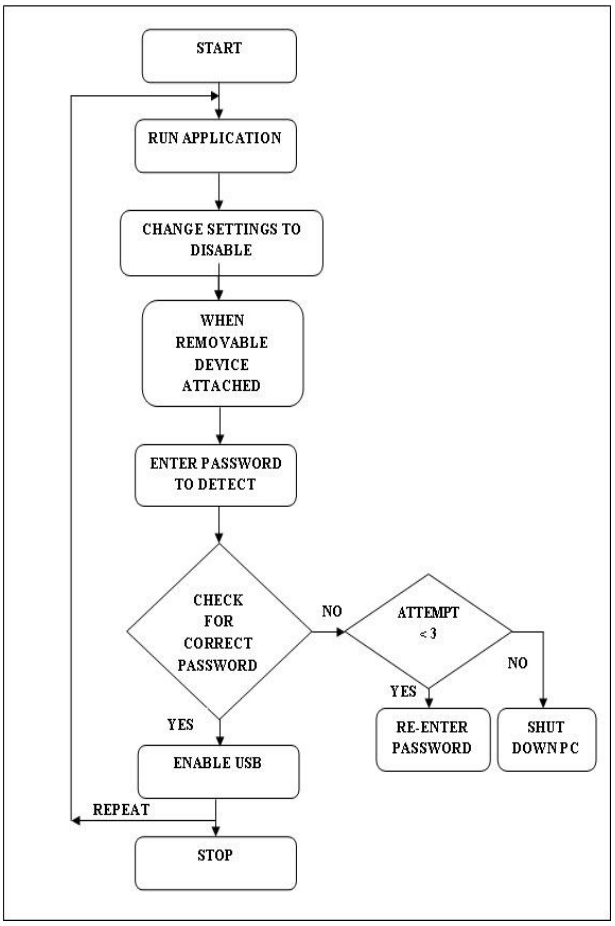

Fig.2 Working Layout

If user selects option ENABLE then a textbox for entering password appears. When user enters password, it will get verified against the original passwords already stored in the database, if they are equivalent then only device becomes ready to communicate. If the entered password is not equivalent, then a message box will display saying "Incorrect Password!!!" as an alert. Client is given three opportunities to enter secret word once more. If neither of the entered passwords are equivalent, then system will automatically shutdown.

If user selects option disable then no device can be accessed unless user prefer enable option and enters the authorized password.

4. FUTURE ENHANCEMENT

In future, improvement can be made to the removable device locker solution package like it can be used to detect virus in external devices. It can also be used to identify particular user individually. Authentication mechanisms similar to face detection or speech recognition can be used to amplify the protection level.

5. CONCLUSION

Removable devices are globally recognized hardware standard of communication, to transfer computer data from one computer to another, whenever needed. But, as the removable devices are increased exponentially the percentage of the removable drives infected by viruses has also increased concurrently. Removable drives can be used to copy sensitive data from computer as well as can be used to spread virus. As there is no guarantee, to ensure removable drives being affected by virus Removable Device Application Lock is developed.

The foremost principle of this paper is for two vital things, first is to grant protection to the computer system from unauthorized user which may connect with the help of USB mass storage devices. Second thing is that this paper basically concepts focus on USB mass storage devices, because of the more possibilities of danger occurrence in the computer system through USB mass storage devices like Pen Drives. This solution package with security password will secure your information as well as your computer system. This paper mainly focuses on security issues in terms of access prevention for an unauthorized user.

References

1) Mr. Ranjith M, Mr. Manjunath C R, Mr. Prasanna Kumar C, " Blocking USB Drive from Virus Using Filtering Techniques", in , "International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)", ISSN: 2278 – 1323, Volume 4 Issue 7, July 2015, pp 3155- 3157

2) Vishal Mali, Lakhan Jadhav, Namdev Chame, Prashant Inje, " Windows Growing Security", in "International Research Journal of Engineering and Technology (IRJET)" e-ISSN: 2395 -0056 , p-ISSN: 2395-0072, Volume: 03 Issue: 03, 2016

3) Durgesh Kumar, Rohit Goel, "Protection to the Computer System from USB Port Devices except Operating System Security: Theory and Development", in "International Journal of Advanced Research in Computer Science and Software Engineering", ISSN: 2277 128X, Volume 4, Issue 2, February 2014, pp 56-59

4) Sun-Ho Lee, "The Study on The Security Solutions of USB Memory", 978-1-4244-5130, 2009 IEEE.

5) Juan-hua, Zhu; Ang, Wu; Kai, Guo,"PC Lock Software Design Based On Removable Storage Device and Dynamic Password", in "2nd International Conference on Computer Engineering and Technology Journal", Vol. 3, 2010.

6) Tushar B. Kute, Kabita Ghosh, "USB Storage Device Control In Linux".