Removable Drive Blocker Application for Virus Detection

[1]K.G.Kharade, [2]R.K.Kamat, [3]R.R.Mudholkar, [4]S.K.Kharade

[1, 4]Assistant Professor, [2,3]Professor
[1]Department of Computer Science, [2, 3]Department of Electronics, [4]Department of Mathematics
Shivaji University, Kolhapur, Maharashtra, India
Email - [1] kabirkharade@gmail.com.com, [2]rrk_eln@unishivaji.ac.in, [3]rrm_eln@unishivaji.ac.in ,
[3]shraddha.k.kharade@gmail.com

Abstract: *Removable drive requires less user interface to install on a system than other types of hardware devices. They have become the most common means of storing data. They can store large amount of information as well as malwares. Removable drive has turn out to be a new transporter in spreading computer viruses. Whenever a malicious removable drive containing malwares is attached to computer, it can corrupt data or the whole system. With the necessity to protect system from removable drives containing malwares, Removable Drive Blocker came into existence. It will detect virus with the help of antivirus software present on the screen and will block the device immediately*

Key Words: *Antivirus, Malicious, Malwares, Removable drive, Virus.*

1. INTRODUCTION:

In recent days the removable drives have become the most excellent device for storing the data. Along with storing sensitive data, these drives can also store harmful viruses. Computer viruses are manmade destructive computer programs which are purposely made to contaminate computer systems and cause trouble for innocent computer users. Hence removable drives have become one of the most common means of malware attacks on computers for the last few years. These computer viruses propagate themselves without user's consent. It spreads automatically infecting the entire system and spreading to other connected systems. The greatest security risk of Removable Drive is traditional malware to spread. The drive is not but it can contain files that are malicious in nature.

Various software's known as anti-virus are available in market. These are used to detect and remove viruses from the computer system. The major role of an anti-virus is protecting file by being affected by viruses, virus scanning and detection, removing virus from infected files and recovering damaged files and objects. They employ different techniques to detect viruses for providing security to computer system. Antivirus software's can detect known virus properly but in case of unknown viruses they are not that much strong. Whenever a removable drive is attached to a computer system anti-virus software is activated. This software scans the whole drive and if any virus is detected then it is removed\repaired. While this process of scanning a drive is in route the user can open the drive. It means that before detection of virus user can open the drive which will lead to spread the virus, thus corrupting the whole system. Due to this reason Removable Drive Blocker application came into picture.

It is an application which consists of enable/disable facility for removable drives. This application needs anti-virus software installed on the computer, it must be updated also. When user connects removable drive to machine, anti-virus software will start inspecting the drive. Removable Drive Blocker application will not allow the user to open the drive unless the drive is fully scanned. After the detection of viruses and on their successful repair the removable drive will be enabled. This application will take help of anti-virus software's log file which contains data related to removable drive scan. Anti-virus software's are not capable to repair all the viruses. This application will block the drive immediately as soon as it detects un-repaired virus

2. LIMITATION OF CURRENT ANTIVIRUS:

Anti-virus Detection Methods have a few chief problems. Most of techniques are better against known viruses and not good against unknown viruses. They take more amount of time to scan a drive for viruses. Antivirus software's database must be updated very often to stay effective

3. FLOWCHART:

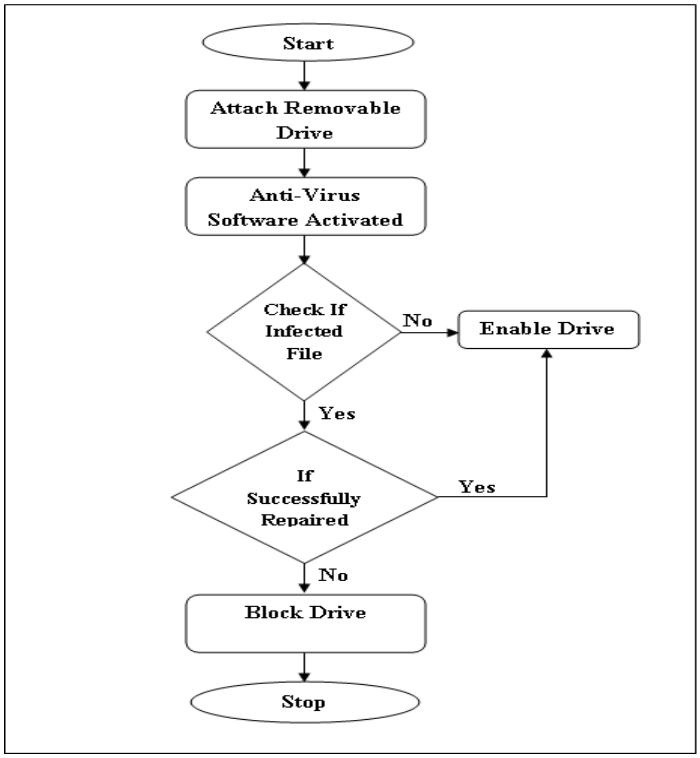

Fig.1 System Flow

First install the application on the computer. User's computer needs an updated anti-virus database in order to successful accomplishment of this software. When a removable drive is attached Removable Drive Blocker Application starts its working. At first it restricts drive so that user cannot open the drive. Updated anti-virus software present on the computer scans the whole drive. This application fetches this log file consisting data related to removable drive scan. If any virus is detected then the anti-virus tries to repair it. After successful removal of viruses the application enables the removable drive and user can open and start using it. If anti-virus software is not able to fix the virus present in the device then the application will restrict access to removable device. The basic system flow is shown in Fig.1 above**.**

4. CONCLUSION:

As the number of removable drives has increased, the percentage of the removable drives being infected by viruses has also increased simultaneously. The convenience of USB from a user's perspective also makes it convenient for an attacker [6]. Anti-virus software can help against some known viruses but are not complete solutions. As there is no guarantee, to ensure that anti-virus software will repair all the viruses in removable drive. The proposed Removable Drive Blocker solution package helps to secure computer system from unrepaired viruses by anti-virus software present on the system

REFERENCES:

1. Essam Al Daoud, Iqbal H. Jebril and Belal Zaqaibeh,(September 2008), "Computer Virus Strategies and Detection Methods", in "Int. J. Open Problems Compt. Math.," Vol. 1, No. 2, pp 30-36.
2. Mr. Ranjith M, Mr. Manjunath C R, Mr. Prasanna Kumar C,(July 2015), " Blocking USB Drive from Virus Using Filtering Techniques", in "International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)", Volume 4 Issue 7, pp 3155-3157.
3. Qiuting Jia, Guizhen Wang, Ruilian Hou, "A USB Flash Disk Viruses Preventing Technique Based on Filtering Access" , 978-1-4244-7237-6/$26.00 C 2010 IEEE.
4. Fuw-Yi Yang, Tzung-Da Wu, And Su-Hui Chiu, (November 2010), "A Secure Control Protocol for USB Mass Storage Devices",in "IEEE Transactions on Consumer Electronics", Vol. 56, No. 4,.
5. M. Bailey, J. Oberheide, J. Andersen, Z. M. Mao, F. Jahanian, and J. Nazario, (2007), "Automated classification and analysis of internet malware", In Proceedings of the 10th Symposium on Recent Advances in Intrusion Detection (RAID'07), pp 178–197.
6. Adrian Crenshaw, "Plug and Prey: Malicious USB Devices", Presented at Shmoocon, 2011.
7. Umakant Mishra, "Methods of virus detection And their limitations".
8. Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade, (March 2014), " Study and Comparison of Virus Detection Techniques", in " International Journal of Advanced Research in Computer Science and Software Engineering", ISSN: 2277 128X, Volume 4, Issue 3, pp 251-253.