USB MONITORING SYSTEM AND SURVEILLANCE

Rajat A. Walke [1], Prof. Jogi John [2], Palash A.Bambodkar [3], Kajol Chaudhari[4], Kashmita Mehar[5]

[1]*(rajatwalke07@gmail.com, PCE Nagpur / RTMNU, India)*
[2]*(jogi.john1@gmail.com, CSE Dept , PCE Nagpur / RTMNU, India)*
[3]*(palasha.dbzgt@gmail.com, PCE Nagpur / RTMNU, India)*
[4]*(kajochaudhari93@gmail.com, PCE Nagpur / RTMNU, India)*
[5]*(kashmitamehar6477@gmail.com, PCE Nagpur / RTMNU, India)*

Abstract: *In this modern computer time it is need to protect our computer system from unauthorized user and application (like viruses) which may crash your computer system or may steal your personal data. This event can be performed by connecting any mass storage (external storage device) like PEN DRIVES etc. thus we should need such type security technique which provides a secure platform to the administrator and installed silently & hidden from users like Key Logger Software. At this platform, provide a software application having password filter interface which keep out to all the USB Port devices from your computer system. The motivation comes from some practical problems which are noted above. Whenever you or anyone put on hold their computer (Desktop or laptop), then any one can copy your system data or many types of viruses comes in your computer if you have no any powerful antivirus then your computer may be crash or your important files may damage. Actually, through this paper presenting that this software provide interface with two options for filtering (Enter password with 2 options). First is, user can enter Administrative Password or secondly enter Software Password. Software Password means that when very first admin install this software that time an interface comes for creating a password i.e. Software Password.*

Keywords - *PMS, Remote Task, Task Manager*

I. INTRODUCTION

This software is used to protect the system data to unauthorized user. It is system group policy software with more security and reliability. This software do not allowed transferring files from system to pen drive without administrator permissions. The user plug a pen drive in system without knowledge of administrator the USB Mass Storage Device is blocked automatically and send plugins the pen drive information about plugins time, device name, serial number, system name, product name to Administrator. If the administrator checkout the information then enable the client system USB Mass Storage Device.

II. PROJECT ANALYSIS

Firstly, it is something needed to be aware that how any USB port is identified by operating system when it connects with an USB device on multiport hub. It is clear that when any device is connected through USB then the Microsoft Operating System Feature Descriptor (Microsoft define a set of vendor specific USB descriptor) get the description of that particular device. This information is used to check the compatibility with computer system hardware as well as operating system. At this point, this software gets description of USB devices from Microsoft operating system feature descriptor (MSOSFD). This algorithm basically proposed for understanding that how the occurrence of a filter, if any signal from MSOSFD become positive.
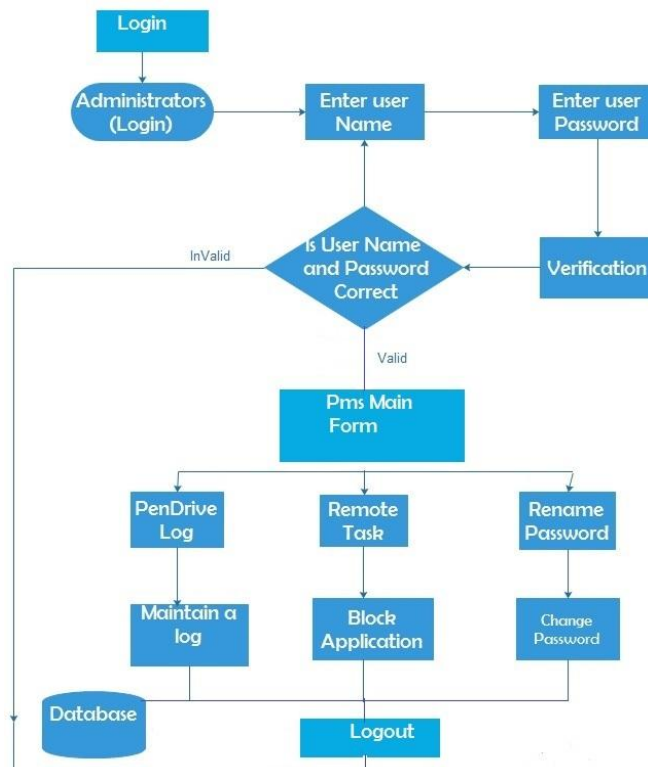
III. DESIGN

Fig 3.1: System Flowchart of USB Monitoring System.

IV. CLIENT AND SERVER

In this project coding is done on both sides, a network has to be set up to connect all the client PC's to the server. Server has the authority to remotely manage all the clients. System Restore properties are used for remote task. All the logs of the USB device will stored in the server machine. Logs include name of the device, size of the disk, available size, IP address of the client. Server machine can access task manager of client machines. It uses some properties of system32 folder of the server machine. Server machine can also turn off, switch user, log off the client machines remotely. It can also enable and disable usb ports of the client machine. It can block any application from client machines remotely

V. SNAPSHOTS

Fig 5.1 : Login Form
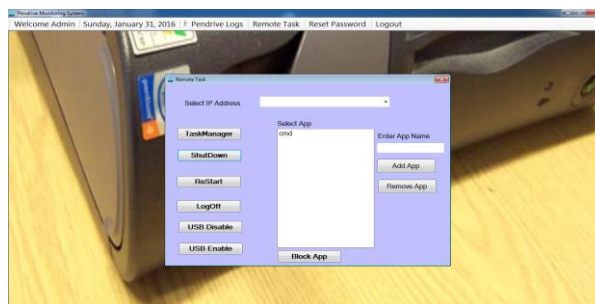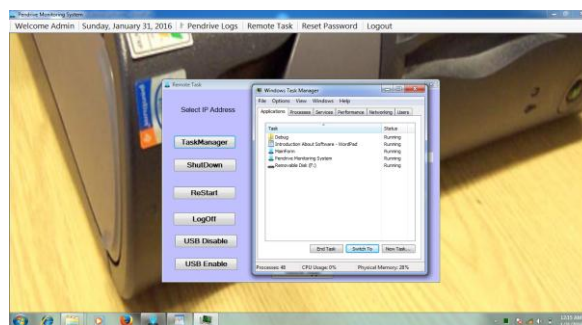
Fig 5.2: Main Form

Fig 5.3 : Remote Task

Fig 5.4 : Task Manager

VI.   CONCLUSIONS

USB Monitor is a basic tool for monitoring and analyzing USB devices and any kind of application working with them on Windows platform. Universal Serial Bus Monitor allows you to intercept, display, record and analyze USB protocol and all the data transferred between any USB device connected to your PC and applications. It can be successfully used in application development, USB device driver or hardware development and offers the powerful platform for effective coding, testing and optimization.

3.1 Limitations
1. **Client Server connectivity must be strong for   this system.**
For running the usb surveillance systems we required the strong connectivity for connecting the server machines to client machines
2. **Currently there is no provision to take a perfect snap of user.**
In this system we have not provision to taking   the snap of user who is connecting the usb devices to machines.

3.2 Purpose
First is to provide security to your computer system from unauthorized user which may connect with the help of USB mass storage devices or you can say that when you do not want to share your data without your permission with other persons. Second thing is that these systems basically concepts focus on USB port type second to monitor the client machines in network. Thus, I believe that this will be more efficient work with usb devices for your computer system.

ACKNOWLEDGEMENTS

REFERENCES

Journal Papers:
[1].   Protection to the Computer System from USB Port Devices except Operating System Security: Theory and Development www.ijarcsse.com/docs/papers/Special_Issue/icadet2014/Lord_14.pdf.

Proceedings Papers:
[2].   Lubonski, M. Gay, V. Simmonds, "A Conceptual Architecture for Adaptation in USB Services Driven by the User Perception of Multimedia" University of Technology Communications, 2005 Asia-Pacific Conference on 03-05 Oct. 2005.
[3].   CaiLongzheng,Yu Shengsheng,Zhou Jing-li, "Research and Implementation of Remote Desktop Protocol Service Over SSL VPN," scc, pp. 502-505, Services Computing,2004 IEEE International Conference on