International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-4, Issue-3, March 2018 Pages 143-146

Secure Copier

Aravindhan.S, Sundar.R, Naveen.D, Raja.R

***Abstract*— Secure copier is a software/ tool which allow the transfer of data between the authorized devices with user's confirmation. A file system is used to cross check whether the pen drive is authorized. Once the pen drive is authorized it checks for jar file inside Pen drive, if the jar file is present in the pen drive it automatically attach a virtual hard disk. All the user action is takes place only inside that Virtual Disk. The Virtual Disk will be attached only to an authorized system. All the operation inside the Virtual Disk is done with user confirmation, in order to avoid transfer of wrong file/data. If the jar file is not present in the pen drive, it automatically recognize that the pen drive is an unauthorized, then the pen drive gets formatted automatically and it ask user confirmation to make it as authorized pen drive with security password. If the user doesn't want to authorize the pen drive, it automatically gets ejected from the system.**

The tool named Secure Copier, inside the pen drive will cross check, whether the system is authorized or not. If it is not authorized system then the tool will automatically format the pen drive.

***Index Terms*—Authentication, Data Confidential, Format Automatiacally , Java Archive , User Confirmation , Virtual Disk.**

I. Introduction

Pen drive is referred as USB flash drive which is a portable device it allows user to transfer data (text, images, video etc.) to and from computer or system. Secure Copier is a tool inside the pen drive (or) flash drive which allows only authorized access to read or write data into device. The device gets formatted automatically when an unauthorized access is detected. This is done by programming into the pen drive which cannot be reprogrammed by hackers to act as HID (Human Interface Device) and custom Keystroke. Here the required details of system and device will be stored in an encrypted format. It uses AES 256bits (Advanced Encryption Standard) encryption technique for storing details where the hackers cannot break easily. The tool automatically decrypts the details. In computing, the USB human interface device class (USB HID class) it specifies a device class for human interface devices such as keyboard, mice, game controllers and alphanumeric display devices. Secure Copier will provide the data transfer between system and device with user confirmation. The data's in secure copier will be more safe because if unauthorized access is detected the device get formatted automatically.

S.Aravindhan, Computer Science and Engineering, KGiSL Institute Of Technology, Coimbatore, India
R.Sundar, Electronics and Communication Engineering, KGiSL Institute Of Technology, Coimbatore, India
D.Naveen, Computer Science and Engineering, KGiSL Institute Of Technology, Coimbatore, India
R.Raja (A.P), Computer Science and Engineering, KGiSL Institute Of Technology, Coimbatore, India

II. OBJECTIVE OF THE PROJECT

A. Platform Independent

This project will be able to run on multiple operating system Submit your manuscript electronically for review.

B. Encryption /Decryption

User will have the privilege to encrypt their files or folders in the mass storage device.

C. Secure File Transfer

Whenever the file is being transferred to or from the thumb drive there will be pop-up with check boxes asking user's confirmation before the actions to be done.

D. Format on unauthorized machines

A Secure Copier tool inside the pen drive check whether the relevant Secure Copier Software is running on machine, if not the tool will automatically format the pen drive.

III. SIGNIFICANCE OF THE PROJECT

- Secure Copier is Software that is used to protect the any type of data from unauthorized users.
- If the authorized pen drive is connected in authorized system , the data transfer will take place
- If the unauthorized pen drive is connected in authorized system, the tool will format the device automatically.

IV. FUNCTIONAL REQUIREMENTS

The Secure Copier project needs have its own needs to work adequately. The main areas of its component include:

- USB Detection
- VHD
- Authorized
- Un-Authorized

A.USB Detection

The Universal Serial Bus (USB) is technology that allows a person to connect an electronic device to a computer. It is a fast serial bus. USB connects different devices using a standard interface. Most people use USB for computer mice, keyboards, scanners, printers, digital cameras, and USB flash drives.

- It check for a file system used by Secure Copier
- Once VHD has verified, It checks the jar file inside pen drive
- Only both the combination get true the USB get Detected

B. VHD

The Virtual Hard Disk (VHD) format is a publicly-available image format specification that allows encapsulation of the hard disk into an individual file for use by the operating system as a virtual disk in all the same ways physical hard disks are used. These virtual disks are capable of hosting native file systems (NTFS, FAT, exFAT, and UDFS) while supporting standard disk and file operations. VHD API support allows management of the virtual disks. Virtual disks created with the VHD API can function as boot disks.

C. Authorized

- If the pen drive and the system is authorized, it calls a jar file inside the Secure Copier Pen drive.
- Once the above operation done, Virtual Hard Disk (VHD) is get attached to the system.

D. *Un-Authorized*

If the pen drive is connected to a Un-Authorized system, USB connection is refused. At the same time data in the pen drive get's formatted automatically.

V. SOFTWARE SPECIFICATION

FRONT END & BACK END

The front end fully designed using java which also includes other efficient tool for effective design.

A. JAVA

Java is a class-based and object-based programming language. Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to byte code that can run on any Java virtual machine and the principles are:

□ High performance
□ Robust and secure
□ Architecture-neutral and portable
□ Interpreted, threaded and dynamic

B. PYTHON

Python is an interpreted high-level programming language for general purpose programming. Python (including C, Python) include a read–eval–print loop (REPL), permitting them to function as a command line interpreter for which the user enters statements sequentially and receives results immediately. Some of the benefits of programming in Python include:

□ Presence of Third Party Modules
□ Extensive Support Libraries
□ Open Source and Community Development
□ Learning Ease and Support Available
□ User-friendly Data Structures

VI. THE PROPOSED SYSTEM

The proposed design aims at Security which allows the transfer of data between the authorized devices with user's confirmation. A file system is used to cross check the pen drive is authorized or not. Once pen drive is authorized it check whether there is an jar file inside the Secure pen drive , If Jar file is present on pen drive it attach the virtual hard disk and all the user operation is take place only inside the pen drive. When un-authorized pen drive gets connected it asks to be authorized with security key if not pen drive get ejected. If the pen drive recognize the system is un-authorized the secure pen drive get formatted automatically

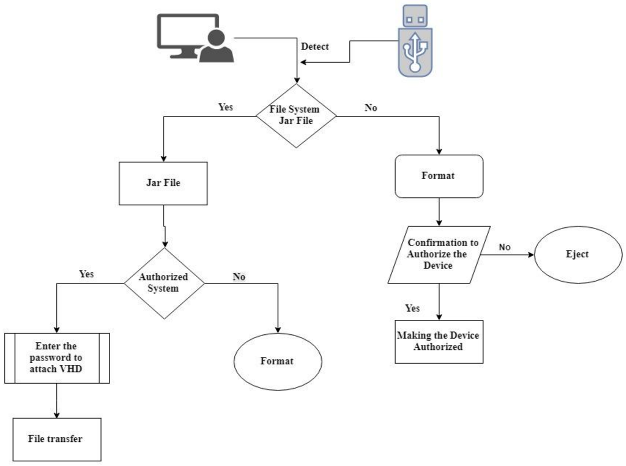

Detect
File System Jar File
Yes
No
Jar File
Format
Authorized System
Yes
No
Confirmation to Authorize the Device
No
Eject
Yes
Enter the password to attach VHD
Format
Making the Device Authorized
File transfer

Fig 1 : **Block diagram**

The design module split is:

Module 1: Authentication Module
- Identify or Detect the mass storage device
- Check for Authorization

Module 2: Add USB Module
- Formatting the USB with specific file system
- Creating Virtual Hard Disk

Module 3: Virtual Hard Disk
- Authentication
- Attaching the Virtual Hard Disk

Module 4: Read or Write Module
- Monitor the events of USB
- Trigger the read or write events if occurs

Module 5: Data Security
- Encryption or Decryption process

When un-authorized pen drive is plugged in to any authorized system, the authorized system detects that missing of jar file and file system, so secure copier tool format the pen drive in particular format and it ask user to want to make it as an authorized pen drive.

When user gives correct security password the pen drive is make it as authorized or else automatically pen drive get eject from the system.

A. Design of software process

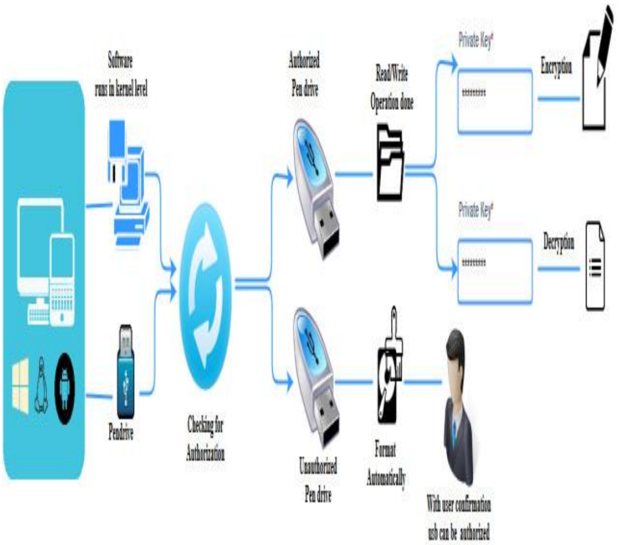


Fig 2 *System flow design*

The design of Implementation is the phase of the project where the theoretical design is turned into a working system. If it is not carefully planned then it can cause confusion. Proper implementation is essential to provide a reliable system to meet the organization requirements. The process of putting the development system is actual use is called system implementation. The system can be implemented only after through testing is done. The system personal check the feasibility of the system. The most crucial stage is achieving a new successful system and giving confidence on the new system for the user that it will work efficiently and effectively.

- ***SYSTEM SIDE IMPLEMENTATION***

Secure copier tool is generated as an executable file and it need to be installed on every Authorized system. The Executable file starts to run, whenever pen drive is plugged into the system, and the important program files will be in hidden mode.

The executable file contains :

□ *Verification process of authorized pen drive*

□ *Making new pen drive as authorized one.*

□ *Creating Virtual Hard Disk to make as authorized pen drive.*

□ *Encryption / Decryption process.*

- ***PEN DRIVE SIDE IMPLEMENTATION***

An un-readable/un-accessible jar file is present on every authorized pen drive. When the pen drive is plugged into system, jar file in the pen drive cross check with Secure Copier tool in system whether the system is authorized, if it is authorized VHD will be attached for user transferring the data securely. Otherwise the pen drive get formatted automatically.

Jar file contains :

□ *Specific File for authorization*

□ *Secure Copier Software*

VII. SYSTEM TESTING

Software testing is an investigation conducted to provide stakeholders with information about the quality of the software product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include the process of executing a program or application with the intent of finding software bugs and verifying that the software product is fit for use.

Software testing involves the execution of a software component or system component to evaluate one or more properties of interest. In general, these properties indicate the extent to which the component or system under test.

A. INTEGRATION TESTING

Integration testing (sometimes called integration and testing, abbreviated I&T) is the phase in software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before validation testing. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

B. COMPATIBILITY TESTING

Compatibility testing is a non-functional testing conducted on the application to evaluate the application's compatibility within different environments.

It can be of two types - forward compatibility testing and backward compatibility testing.

□ *Operating system Compatibility Testing - Linux , Windows*

□ *Database Compatibility Testing - Oracle SQL Server*

□ *Browser Compatibility Testing - IE , Chrome, Firefox*

Flash drive check for the following condition's :

- Authorized system
- Unauthorized pen drive
- Unauthorized system

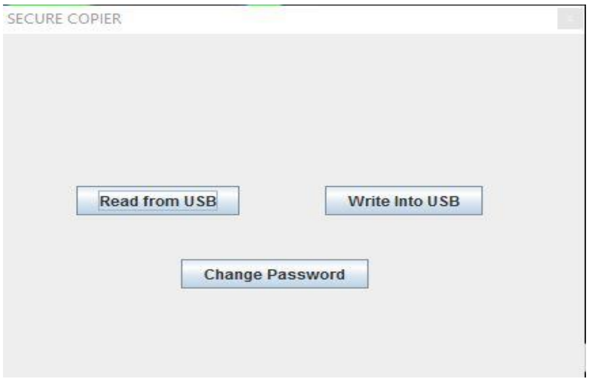
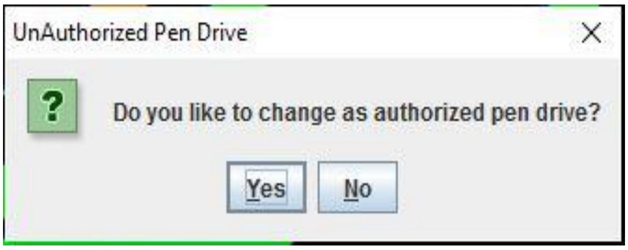


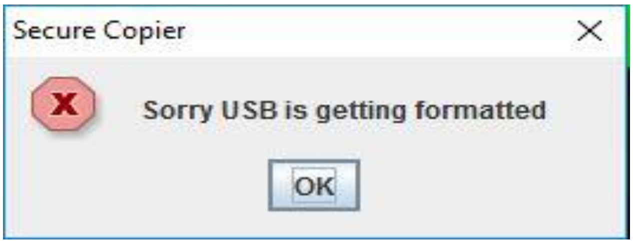
FIG 3 : Authorized system login access



UnAuthorized Pen Drive

Do you like to change as authorized pen drive?

FIG 4 : UnAuthorized pen drive access permission



Secure Copier

Sorry USB is getting formatted

FIG 5: Unauthorized system format drive automatically

VIII. CONCLUSION AND FUTURE WORK

The Secure Copier project has been done to transfer confidential data securely and safely within the division or organization. The Software will allow only authorized devices to be enabled on machine. Meanwhile if the device is connected to any unauthorized system, it gets formatted automatically. So the data inside the device will be more secure and intruders cannot read or steal the data. This software will be more useful in defence and also the area where they need to transfer confidential data of any size. The data transferred using Secure Copier tool will be stored encrypted in the device. The tool will help the user to transfer data with user confirmation, so no data will be copied without user knowledge. This tool will prevent from affected files and virus files. The tool will be more user friendly to users and all operations are automatic.

REFERENCES

[1] Fuw-Yi Yang, Tzung-Da Wu, and Su-Hui Chiu, “A Secure Control Protocol for USB Mass Storage Devices”, IEEE Transactions on Consumer

[2] Kyungroul Lee, Hyeungjun Yeuk. “Safe Authentication Protocol for Secure USB Memories”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 1, pp. 46-55, December 2010.

[3] Oracle, “Kinds of compatibility,” Online: https://blogs.oracle.com/ darcy/entry/kinds of compatibility (Jan, 2015).

[4] K. Zetter, "An unprecedented look at Stuxnet the world's first Digital weapon", *Wired*, 2014, [online]

[5] "Turning USB peripherals into BadUSB", *Security Research Labs*, 2014

[6] D. Wagenaar, D. Pavlov, S. Yannick, "USB baiting", *Universite van Amserdam*, 2011.

[7] S. Wright, "Honey stick project - phase 1 results", *Streetwise Security Zone Tech. Rep.*, 2012

[8] J. Larimer, "USB autorun attacks against linux", *Hackito Ergo Sum 2011*, 2011.

[9] K. Nohl, S. Krissler, J. Lell, "BadUSB-on accessories that turn evil", *Black Hat USA*, 2014