**Secure pendrive copier**

**Abstract**

Secure copier is a software/ tool which allows the transfer of data between the authorized devices with user’s confirmation. An virtual hard disk is introduced in order to encrypt the data automatically and to make it as a secured data storage. Only the authorized machines will be able to read the virtual hard disk on the mass storage device, to access the data. In case of, unauthorized access in authorized system, the tool will format the mass storage device automatically.

**Area Introduction-Existing system**

There are some existing protected USB flash drive:

* IRONKEY
  + Cryptochip (for authentication)
  + Auto-format
  + Expensive than Data Traveler (nearly lakhs)
  + DATA TRAVELER
  + Alphanumeric keypad
  + Full-disk AES 256-bit hardware

based encryption

* + Most expensive (nearly 15000)

**Proposed System**

In this project, the large amount of confidential data will be transferred securely. Only the authorized person can access the data. This project is mainly to prevent data from unauthorized access.

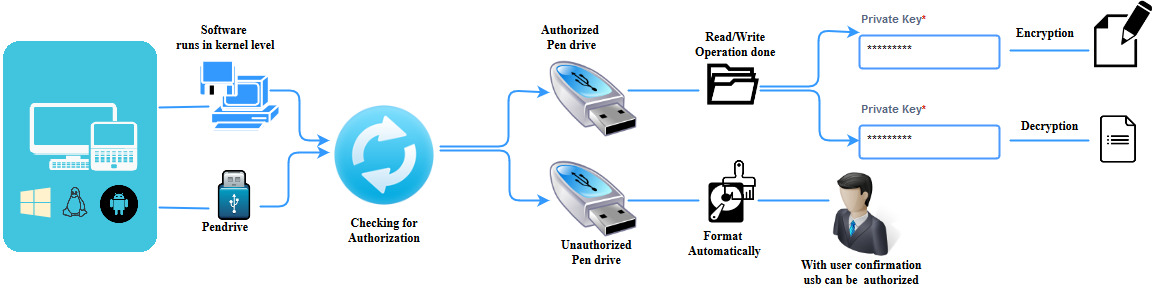
Advantage over existing methods

* No need to depend on particular pen drive or mass storage device.
* Each file will be transferred with user confirmation.
* Stronger Authorization.

Future Enhancements

* Secure Copier will be designed to work on multiple operating systems.
* Authorized pen drive will be defined with the virtual hard disk.
* In order to read or write into the device, the system needs secure copier software.
* If the unauthorized pen drive is connected in authorized system, the tool will format the device automatically.

**Architectural Design**

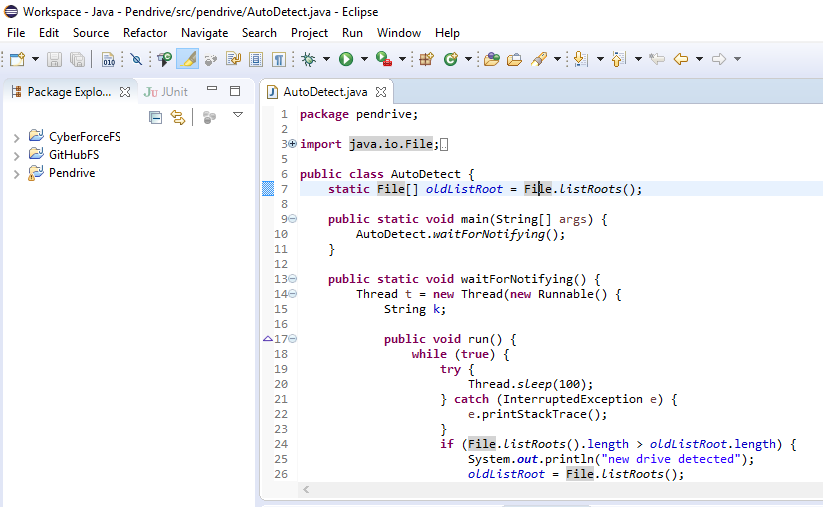


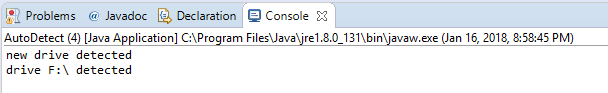
**Module wise development plan or Process Flow Diagram**

****

**Authentication Module**

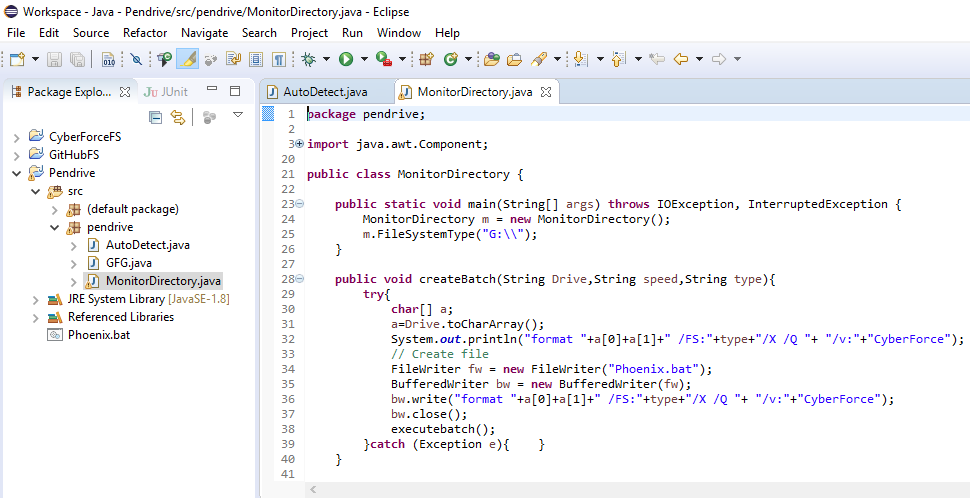
**Coding snippet :**



**Output :  
 **

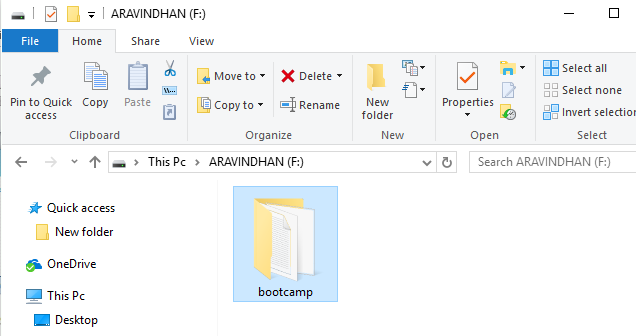
**Read or Write Module**

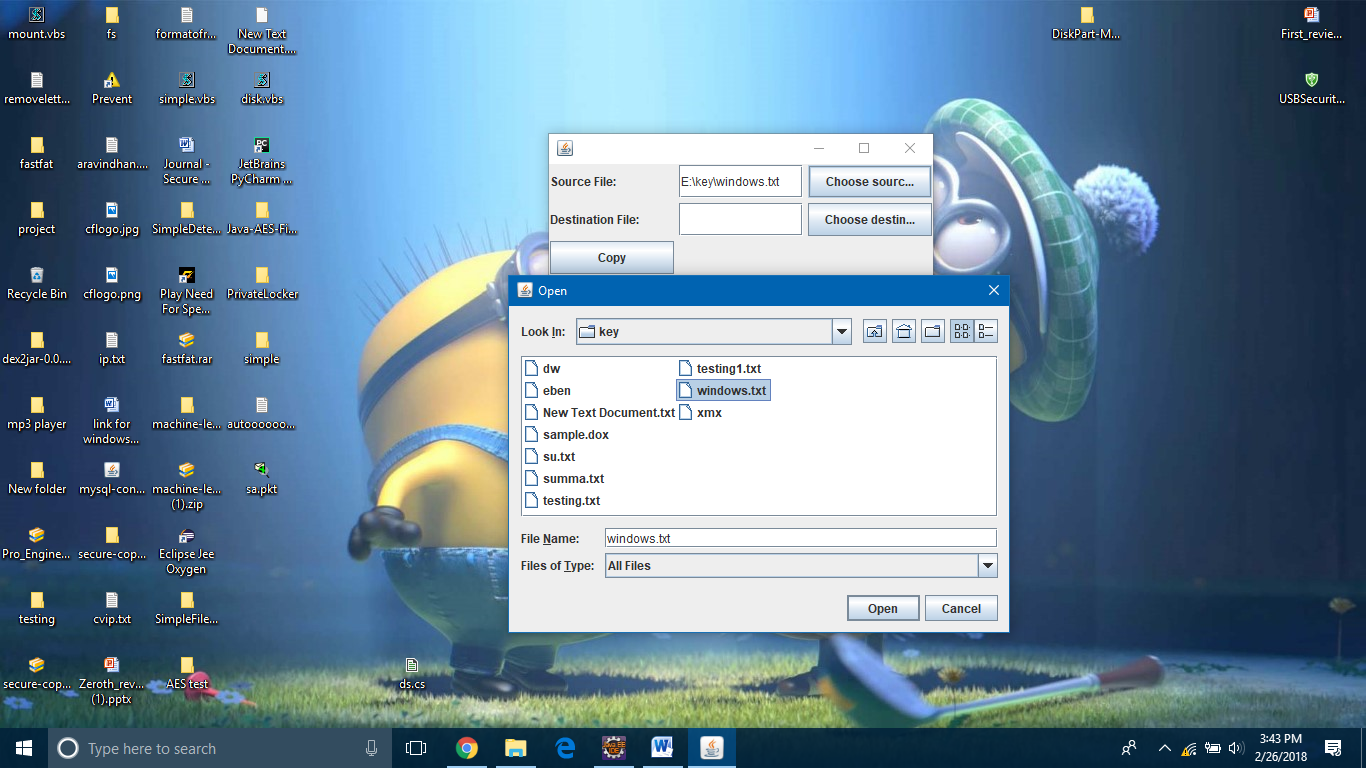
**Coding snippet :**

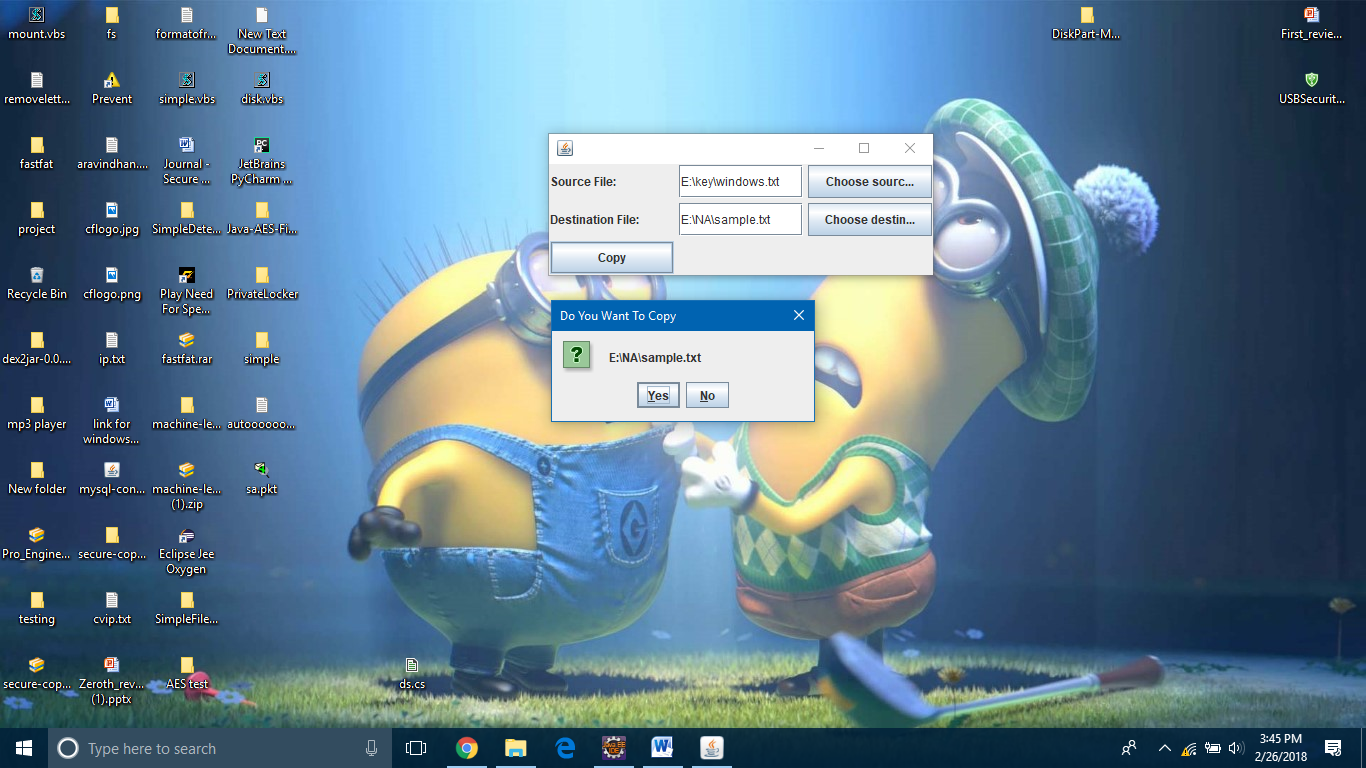
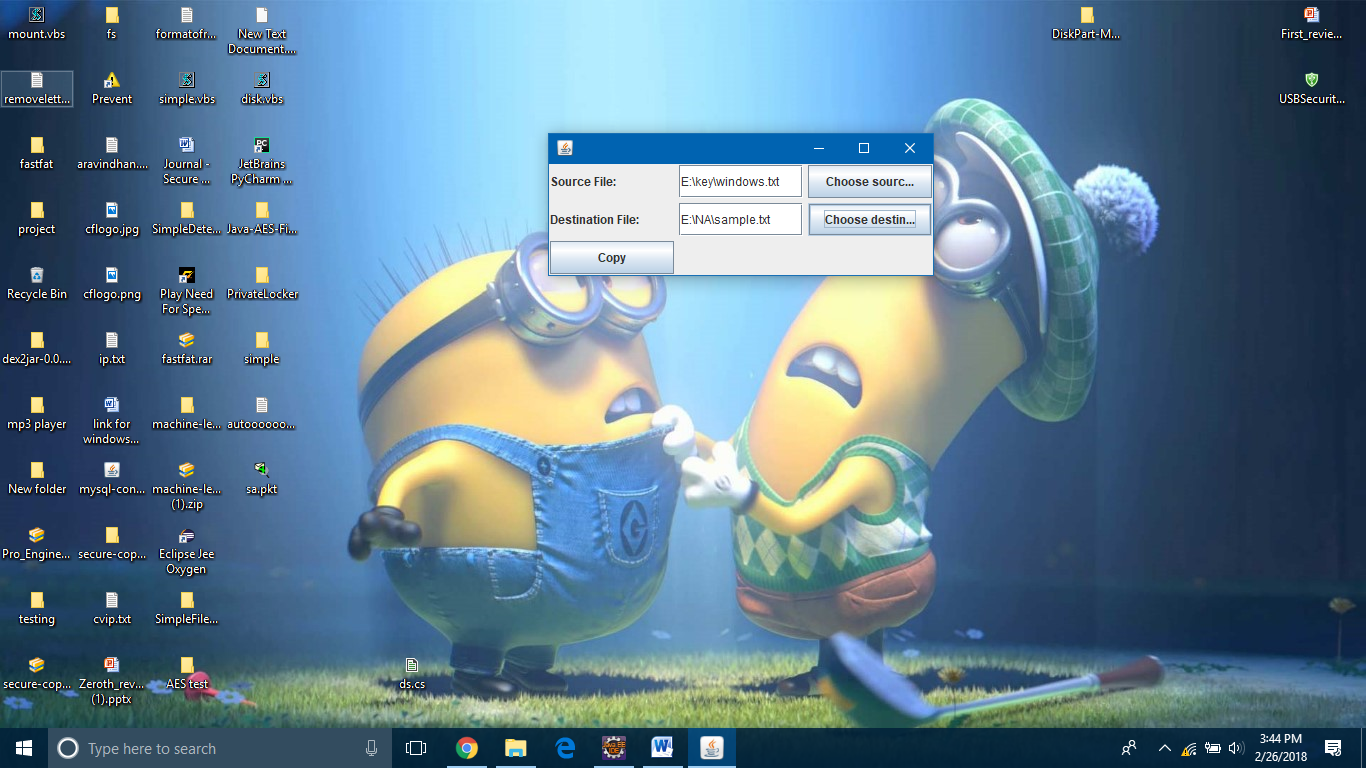


**Output :**

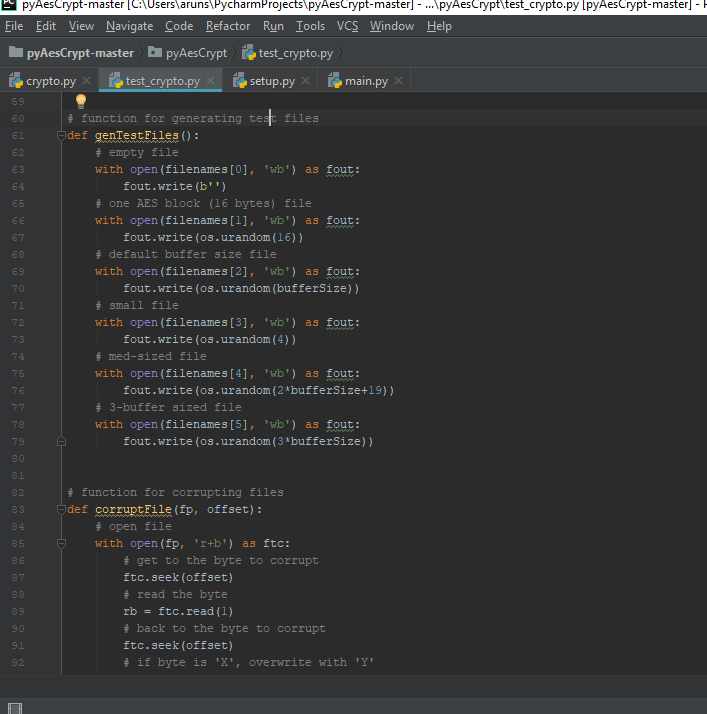
****

****

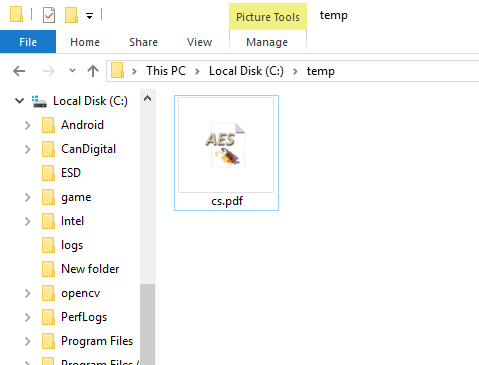
****

****

**Data Security**

****

**Encrypted File :**

****

**Decryption :**

