I J C T A, 9(41) 2016, pp. 1285-1288 ISSN: 0974-5572
© International Science Press

SECURING AN EXTERNAL HARD DRIVE

Rajneesh Tanwar*,K.Krishnakanth Gupta, and Purushottam Sharma***,**

Abstract:We store data in many ways like storing in tapes, floppy, hard drives of both internal &external drives and the new way of storing data is cloud. Though we can't store large amount of sensitive data in cloud due to some security issues we store it in hard drives. Let us assume a worst case that is what if the hard drive is misplaced or got robbed? Though we have password encryption techniques to the drive we need to locate the drive. So, our proposed method gives a solution to this problem.

Key Words: *File systems, Internet of Things (IOT), Self-Encrypting Hard Drive (SED), Cloud Computing*

1. INTRODUCTION

Answer for both wired and remote. By and large the new remote hard drives are equipped for interfacing with one or more gadgets that might be PC, portable or palm tabs which lies an issue called heterogeneity for the product introduced along drivers which are utilized to bring data of the gadget it is associated and we can defeat that issue as well.As we described in the abstract means of storing data is done in many ways like storing in tapes, floopies, hard drives and cloud computing. Tapes and floopies are old way of storing data so we use hard drives and cloud technologies. Though we don't store large amount of sensitive data in cloud due to security and privacy issues we store such data in a hard drives. Though hard drives are not meant to be shareable devices we may lost drives in any kind. So, we have to find out the location of device to retrieve the disk and prevent loss or leak of sensitive data. So here we find out the location devices by adapting the method from the concept of Internet of Things (IOT). IOT is where we connect our daily useful objects to the internet and get control of its functionality and the objects are controlled by end devices like smart phones, notepads, computers etc. so we adapt IOT technique which is sensing and automation to locate the disk and send the information of system which it is connected to.

In today world, for storing huge amount of data any storage unit are available in the market with very low cost and high storing size. High volume products are now a day is need of a common person or citizen as the data is rowing in very big ratio. [2]

Despite the importance of the subject, there are many techniques or paper are formatted and formulated for protection of these devices or protecting data stored inside them [3]. Their data are typically based on extrapolation from accelerated life test data of small populations or from returned unit databases. Advancement in life has also advanced the technology due to till now no good solution for protecting such devices is available in the market. [4]

Disk drives are generally very reliable but they are also very complex components. This basically defines that these devices are very hard and not easy get fails in change of environment. These are very reliable due to which every citizen kept confidential data in it but the main concern is security in which these device have very lose hand. In this paper we are going to build up these device smart enough so that their lose hand in security will going to be strongest part by saving data to be accessed by unauthorized one.[1]

Each hard drive chips away at PC by introducing drivers into PC in which programming drivers are useful to identify any equipment parts and correspond with that equipment gadget. So in hard drives there is chip present called self-Encrypting Hard drive or full circle encryption which controls entering of information or erasing of information into the drive and it has the full control hard drive for scrambling and unscrambling information or passwords and establishment of drivers and so forth here we compose a code to send the data of the pc in which the drive is associated. What's more, this code ought to run independent of working framework and record framework in which the PC is utilizing [5][8][9]. Presently a day there are most recent hard drives which are wired and remote [10] so we give an

2. USE OF INTERNET OF THINGS(IOT) CONCEPT

Generally IOT works on the functionality of sensing and automation[11][12]. Device senses things and sends the information over the internet, if it is connected to internet then the device gets functionality from the user and automation is in which the sensed raw data is used as a useful information. So here we take this functionality and usage of this functionality is described as when we connect the hard drive to computer it install drivers first and second it install a software which gets the information of the computer and the drive ID which is connected to the computer and sends the data to the manufacture of the drive. At the manufacture site they have the list of their product id and their customer’sinformation, if the product id is matched they send the information of computer in which their product is connected. Here generally IOT devices have wireless sensors to sense the things and send data to the user. But in wired hard drives we don’t have any sensing device, it just contains a piece of software which fetches data of a computer like User name, IP address, Mac address of which the drive is connected.

2.1 Self-Encrypting Hard Drive (SED):

Self-Encrypting hard drive (SED) [6][7]is said to be a piece of software and hardware chip in hard drive which are used for the functionality of encrypting, decrypting of data or passwords of a hard drive and it is transparent to the user. It may be Solid State Drive (SSD) or hard disk drive (HDD), wired or wireless devices SED is the main. So we write a programme for the SED to get the information of the end devices in which it is connected. As soon as drivers are installed by the SED it install the software in end devices to fetch the information of that end device and sends to the user via manufacturer. So here Self-Encrypting Hard Drive(SED) plays a major role. This SED works generally irrespective of file system which the end device it is using, so design the software according to it.

2.2 Use of Email services in the computing devices

We have SMTP and POP3 mail services in computing devices, by use of this services we send the fetched data of computing device to the manufacturer and from there manufacturer checks and sends the data to the customer. So by use this we can locate or track the hard drive and prevent from leaking of data and loss of drive.

3. IMPLEMENTATION

Algorithm:

3.2.1 Hard drive connected to computing device which may be wired or wireless.

3.2.2 If an wired hard disk is connected to the computer or a laptop installation of hardware drivers and software that fetch information of computing device

3.2.3 If it is wireless it is connected to n number of devices such as computer/laptop, smart phones, palm tabs etc.

3.2.4 Information about the device is fetched such as username, MAC ID/EMI, IP Address.

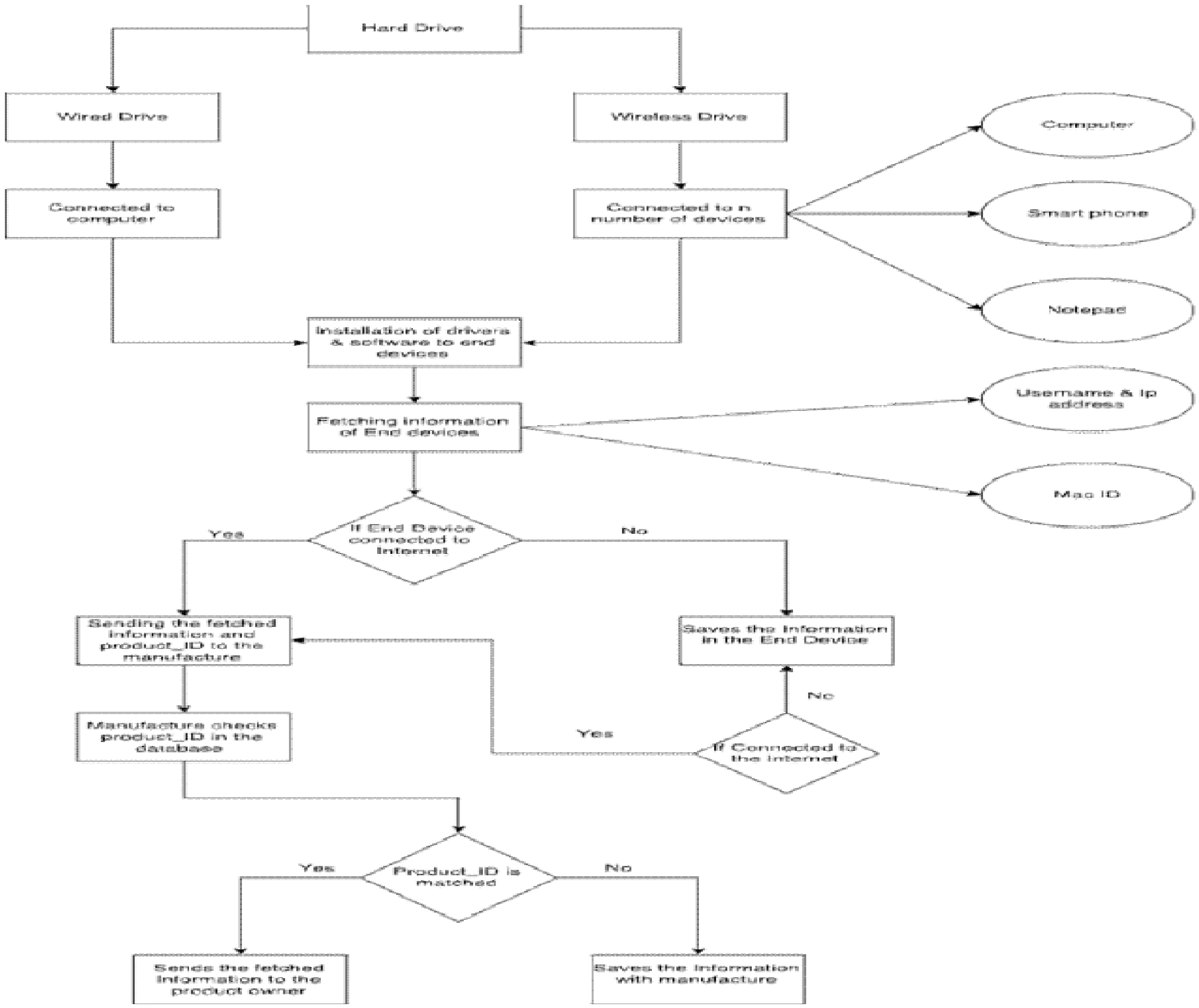
3.2.5 If the end devices are connected to the internet the fetched information is sent to the manufacture along with product_ID of the drive connected to end device.

3.2.6 If the end device is not connected to the internet then the fetched information is stored in the end device itself which will be transparent to the user.

3.2.7 After sending the fetched information manufacture will check the product_ID and sends the end device information to the product owner.

3.2.8 If the product_ID is not with the manufacture it saves the information to find out the person who sent the duplicate messages.

Flow chart:


Hard Drive
Wired Drive
Wireless Drive
Computer
Connected to computer
Connected to n number of devices
Smart phone
Notepad
Installation of drivers & software to end devices
Username & Ip address
Fetching information of End devices
Mac ID
Yes
If End Device connected to Internet
No
Sending the fetched information and product_ID to the manufacture
Saves the Information in the End Device
No
Manufacture checks product_ID in the database
Yes
If Connected to the internet
Yes
Product_ID is matched
No
Sends the fetched information to the product owner
Saves the Information with manufacture

CONCLUSION

In this paper we propose how to secure external hard drive through method of IOT so that external drive can protect even if it was robbed and giving control over the disk by use of computer if it is connected. By this way, whole data in the disk will be safe and all safety measures are taken buy user only and no third party software are used for performing such security in hard disk. So our proposed solution concludes that a hard drive can be secured at the time of worst case by adapting the concept of IOT. We find out the problems and software implementation demo in next discussion.

References

[1] Eduardo Pinheiro, Wolf-Dietrich and Luiz Andre Barroso. “Failure Trends in a Large Disk Drive population“, proceeding of the 5th USENIX conference on the File and Storage Technology , February 2007.

[2] Peter Lyman and Hal R.Varian. How much information? October 2003.

[3] Dave Anderson, Jim Dykes, and Erik Riedel. More than an interface - scsi vs. ata. In Proceedings of the 2nd USENIX Conference on File and Storage Technologies (FAST’03), pages 245 – 257, February 2003.

[4] Jon G. Elerath and Sandeep Shah. Server class disk drives: How reliable are they? In Proceedings of the Annual Symposium on Reliability and Maintainability, pages 151 – 156, January 2004.

[5] http://www.storagereview.com/ssd_vs_hdd

[6] http://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security

[7] https://en.wikipedia.org/wiki/Disk_encryption

[8] http://windows.microsoft.com/en-in/windows-vista/comparing-ntfs-and-fat-file-systems

[9] https://en.wikipedia.org/wiki/File_system

[10] http://www.wdc.com/wdproducts/library/?id=461&type=25&cn=4779-705118

[11] https://en.wikipedia.org/wiki/Internet_of_Things

[12] http://www.microsoft.com/en-in/server-cloud/internet-of-things/overview.aspx