JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING
ISSN: 0975 – 6760 | NOV 16 TO OCT 17 | Volume 4, Issue 2

# ENHANCING SYSTEM SECURITY FROM UNAUTHORIZED USB DEVICES AND EVIDENCE COLLECTION TO PROVE DATA THEFT

[1]MohammadAsif Khan, [2]Tosif Attar
[3]Harshal Deore, [4]Shilesh Patil

[1] asifkhan948@gmail.com
[2] toshi.atr@gmail.com
[3] deoreharshal775@gmail.com
[4] shaileshpp19@gmail.com

Department of Computer Engineering,
Rajgad Dyanpeeth Technical Campus, Pune University,
Dhangawdi Pune- 412205 ,Maharashtra India

***ABSTRACT:***
In day to day life we face many problems related to data theft from external storage devices like USB storage devices. Most of the times peoples are unaware of their data is stolen or what data is stolen and in some cases peoples do not know the person who committed theft and even if they know, they do have no proof of that. In the information age, cybercrime is increased and can leads to intentional/unintentional misuse of such data which causes from mentally harassments (individuals) to serious losses in a business (organizations). This paper addresses the issue of such theft and its various impacts. The system resolves the issues by modifying the current USB access algorithm to identify authorized/unauthorized devices and to on the fly encrypt the data in case of unauthorized devices and at the same time generating alerts through Email and SMS with hostname, device id, photo of a thief etc. to the owner/admin by constantly monitoring the machine(s) for such theft.

***KEY WORDS****: Data theft prevention, Tracking copying of data from system to USB, Data theft prevention from unauthorized USB device.*

## 1. Introduction

The Universal Serial Bus (USB) is a widely used serial cable bus for connecting various peripherals (such as USB storage devices) to a host computer.

Now a day's data theft is major problem, people keep their data (personal/business documents) in a digital (electronic) format and referred as digital data. Portability, easy to copy are the nature of the digital data they are more prone to theft. Data theft is usually perpetrated by anyone who is criminal minded for their own benefits (personal gain) or to harm someone (organizations/individuals). Because of the ubiquitous nature and widespread use of the of USB, it becomes a great tool to carry the data for the person who is going to commit a theft. That is, most of the data is stolen using USB storage devices because they are easy to carry, can hold vast amount of data and can easily connected to almost every kind of devices, and can left almost few traces of data theft but requires experts to find those traces [2].

It is necessary to prevent data theft in order to avoid substantial losses to money, reputation etc. The system proposed in this paper can be used to reduce data theft of individuals, organizations and military organizations as well where the data is highly sensitive and cannot be disclosed.

## 2. Literature Review

S. Verma and A. Singh [1] given a solution where a white list of devices is maintained and only devices present in that white list are allowed and considered authorized and in case of unauthorized devices the ports are blocked to prevent unauthorized devices. The white is present at a centralized repository in a network that is on server and every client keeps the synchronized copy of that white list as a local copy.

A. Ramani and S. Dewangan [2] it gave an overview to carefully investigate the windows 7 registry to track down the traces left after the data theft such as when the suspected USB device is connected and when the last time data is copied etc. that is using windows registry only limited amount of details can be traced and it is sometimes possible to extract some more hidden information.

A. Shastri and P. Sharma [3] it gives separate vault where user can store their sensitive data which

protects from leakage and/or unauthorized access, the vault is responsible for every data retrieval, it provides security to all data within vault no matter whether data is at rest, data in use and data in motion. Without disturbing user's usual workflow.

M. Bhosale and G. Patil [4] it gives users access behavior profiling that is authorized/unauthorized users can be identified by the certain behavioral properties such as attempt towards the user login, timing of login speed of pressing keystroke by logged user, habit of using mouse or keystroke for submitting for using this key parameter check whether the user behavior is normal or suspicious and then blocking/unblocking of the system done.

M. Kang [5] in this paper, there is a middleware present in between USB device and host. The middleware comprises of a hardware kit (such as BBB) and called as USB wall, every communication between USB device and host handled by this middleware kit. It is pretty much costly but provides best solution to prevent data theft and to avoid other harmful malware attacks.

A. Magdum and Y. Patil [6] given a two-layer data transfer algorithm to secure the data transferred to/from USB storage devices. The first layer ensures that only the authenticated user can transfer data to/from USB storage devices, that is first layer is used for authentication while the second layer is used to encrypt the data transferred from host to USB, decrypt the data transferred from USB to host.

F. Yang et al. [7] given a protocol which where a remote authentication server is configured to verify authenticated users and uses the Diffie-Hellmen key technique to protect the data transmitted to a USB storage device

.

## 3. Proposed Work

The vision of the proposed system is not only to track and limit the access of unauthorized devices, but also to collect the evidence to prove the data theft, and to find the person who committed the theft. This system will be kept hidden from the user (most probably the thief) this means only the admin/owner of the system has the access to view the application. Admin can access a hidden console/GUI to register the devices in a white list, to view the logs, to set up email addresses and mobile numbers to receive alerts.

When a system is deployed there will be a monitoring daemon/service which will continuously monitor the system (host machine) for USB devices. And when any USB device is connected to the host the monitoring service will detect the device and it is uniquely identified and then authenticated using white list. If device is authorized, then allow original data else encrypt the data. Generate logs and alerts.

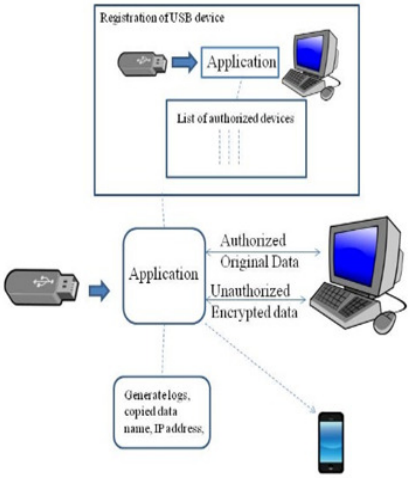


Fig 1: Proposed Architecture

### 3.1 Device Detection

A monitoring daemon/service running in background to listen the USB ports that is to detect the devices plugged/connected to the port and after the detection of the device, a service to for device identification is called.

### 3.2 Device Identification

The USB device should be identified uniquely using unique identifiers such as a combination of VID (Vendor ID) and PID (Product ID) [8]. These ID's are 4 characters hexadecimal ID; e.g. a typical VID and PID looks like VID_xxxx and PID_yyyy respectively, where xxxx and yyyy is a hexadecimal number.

### 3.3 Device Authentication

The list with unique identifiers (such as VID and PID) of all registered devices is maintained in an encrypted form in a database on a host machine and thus referred to as a white list. After the identification of the USB device it is checked whether it is present in a white list or not. If present, the device is considered as an authorized device else the device is considered as an unauthorized device.

### 3.4 Allow Authorized Devices

If device is authorized, and if the user request to copy data from host to USB device then allow it to copy original data or unencrypted data.
If device is unauthorized, and if the user request to copy data from host to USB device then encrypt the data on the go that is apply on the fly encryption to the data being copied without being noticed by the user (most probably the thief). In this case the encrypted data will act as an evidence to prove the data is stolen by the person who possess that data and the main motive of encryption is to collect an evidence and still prevent the thief from accessing the data.

**3.5 Generating logs and Alerts**

At the time of copying data from host to USB device, logs such as data being copied, IP address of host, user id (logged in user), image (photo) of the person in front of the webcam etc. saved on a local machine in an encrypted form. And the same copy of the log is sent through an email to the admin/owner on his/her registered email address and also on mobile phone through SMS (without photo) on real time and if the internet connection is not available then the alerts are sent when the network connection is available. All these logs will act as a proof to prove the data theft and to find out the person who have committed the theft.

**3.6 Algorithm**

3.6.1 *Default USB Access Algorithm*

**Input:**
VID: Vendor ID of USB device
PID: Product ID of USB device
PORT: Virtual port on which device communicating with system
**Output:** Give Access/ Install Drivers

**Algorithm:**
IF VID ≠ 0 and PID ≠ 0 PORT ≠ 0
List L: List of all VID and PID from local.inf file from root directory
FOR EACH item in L (|L| >= 1), do
If item [VID] == VID and item [PID] == PID then
B ←Give Access
IF B == Give Access then
Communicate with plugged USB
ELSE
Install desired drivers then
Communicate with plugged USB

3.6.2. *Proposed Algorithms*

**Input:**
VID: Vendor ID of USB Device.
PID: Product ID of USB Device.
PORT: Virtual communication port of device with system.
Host Name: Get the host name of computer
Login ID: Get digital identity of user
IP Address: Get IP address of computer
**Output:**
Result: Allow original data /Allow encrypted data.

**Algorithm:**

IF VID ≠ 0 and PID ≠ 0
List L: List of all white listed USB devices
FOR EACH item in L (|L| >= 1), do
IF item [VID] == VID and item [PID] == PID then

Result ← Allow original data.
GenerateLog(VID,PID,Host Name,Login ID,IP Address,Image)
Alerting Process (VID,PID,Host Name,Login ID,IP Address,Image)
Else
Result ← Allow encrypted data.
GenerateLog(VID,PID,Host Name,Login ID,IP Address,Image)
Alerting Process (VID,PID,Host Name,Login ID,IP Address,Image)
End

**4. Result Analysis**

**4.1. Result Analysis Throughput**

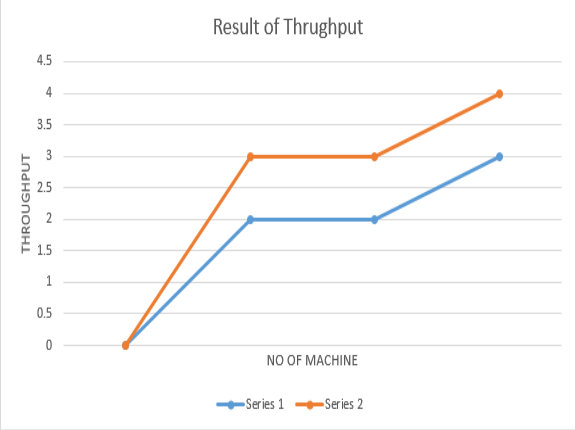


Fig 2: Result Analysis of Throughput

There was no such system available suddenly the administrator when any other person uses his system without his permission and he also not aware when any other person uses his system but our system gives real time notification when any foreign device attach to admin system and also notify that which data has been copy at that time

### 4.2. Result Analysis of Data Copy

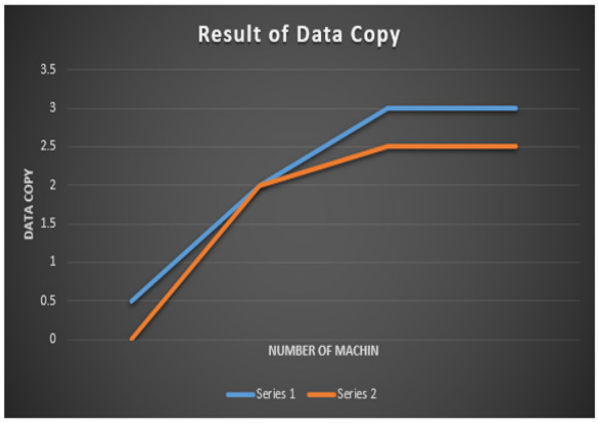


Fig 3: Result Analysis of Data Copy

In previous system we Can't identify who stolen our data, only we identify which data has been we loose and to overcome this drawback we develop such system that identify the person who has stolen our data and he is not able to that data

### 4.3. Result Analysis of Theft Identity

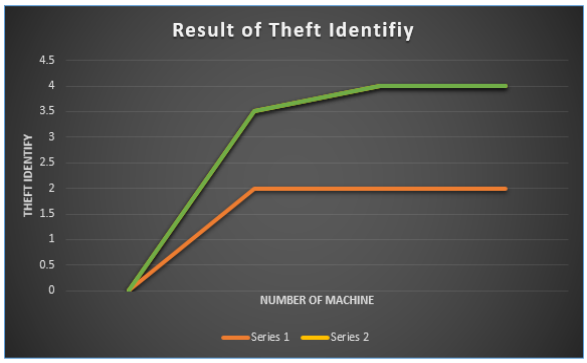


Fig 4: Result Analysis of Theft Identity

In the previous system (safeties endpoint audition gives us all the history. All the details about work of that user his activity of that system The drawback of this system is that it
cant
identify the quality person successfully it just shows the crime activity not identify the criminal to overcome this drawback we built such system that identity the quality person accurately and
we prove that

### 5. Conclusion

Data can be theft from various ways, through various devices but in last few years approximately 70% data (among all reported data stolen) is stolen using USB devices [9], the USB storage devices are the one of the preferred (because of its various cons.) device that are used to steal digital data from individuals' computer or organization's computer. There are thousands of ways to misuse the stolen data and can leads to the disasters things to happen. This paper addresses and provides a solution to reduce such theft to the great extent.

### 6. Acknowledgments

We are grateful to Prof. S. P. Patil for their guidance and support.

### 7. References

[1] S. Verma, A. Singh, "Data theft prevention & endpoint protection from unauthorized USB devices", *IEEE*, 2012.

[2] A. Ramani, S. Dewangan, "Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device", *IJCSIT*, 2014.

[3] A. Shastri, P. Sharma, "Data Vault: A Security Model for Preventing Data Theft in Corporate", *ACM*, 2016.

[4] M. Bhosale, G. Patil, "Insider data theft prevention using behavior profiling", *ICCCES*, 2016.

[5] M. Kang, "USBWall: A Novel Security Mechanism to Protect Against Maliciously Reprogrammed USB Devices", 2015.

[6] A. Magdum and Y. Patil, "An Algorithm to Avoid Confidential Data Theft from Storage Devices", *IJRITCC*, 2014.

[7] F. Yang, T. Wu, and Su-Hui Chiu, "A Secure Control Protocol for USB Mass Storage Devices", *IEEE*, 2010.

[8] vendors and products, http://www USB.org

[9] http://www.darkreading.com/risk-management/how-usb-sticks-cause-data-breach-malware-woes/d/d-id/1099437?