iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Computer Security from External Devices

Pushkar Shetye[1], Chandrashekhar Khot[2], Abhishek Karande[3]
Computer Engineering, Terna Engineering College, Sector 22, Nerul, Navi mumbai.

Abstract— the portable storage market environment is rapidly changing due to the emergence of USB memory. USB memory is used as a portable storage device by many users. However, due to the high portability of USB memory, there are many problems where personal identifiable information data and corporate confidential affairs are leaked to the public in case of loss, theft, or capture of the portable device. Therefore it is very important to develop various kinds of authentication solutions to protect the confidential information against unauthorized access.

In this paper we present the implementation of system that limit access and manage identity for endpoint protection and data theft prevention from USB and external devices to maintain information security in a corporate environment.

I. INTRODUCTION

With the great advancement of Smartphone's technologies and ever increasing ubiquitous access and advances of storage technologies, the corporate and personal data are becoming more vulnerable. The usage of portable devices like iPods, USB sticks, PDAs is becoming commonplace in our society. Also, businesses are embracing new technologies and integrating with World Wide Web to increase productivity. Therefore corporate data are becoming more mobilized and distributed and hence increasing security risk for enterprises. [1] To maintain a rigid protection against data theft in a corporate or personal environment, employee or user behavior must be handled with a highest degree of care. Therefore it is very important to develop various kinds of authentication solutions to protect the confidential information against unauthorized access. The common way is to take off the USB port from the computer to prohibit the use of USB storage devices [2].

II. PROCESS DESCRIPTION

The main aim of this project is to develop various kinds of authentication solutions which will track record and limits the use of USB devices in a secured environment (network) thus maintains confidentiality and integrity to meet information security standards and protect the confidential information against unauthorized access. We are proposing to keep a centralized database of allowed devices such as USB key board, printer, and mobile devices and mouse etc. based on organization's security standards [2]. Along with centralized database, system should keep a distributed database of devices in each local system, and it should be keep up to date by sync mechanism to let system work if central database is not reachable (system is off line).

The process flow [3] of system is shown in following figure for hardware detection is given by following algorithm:

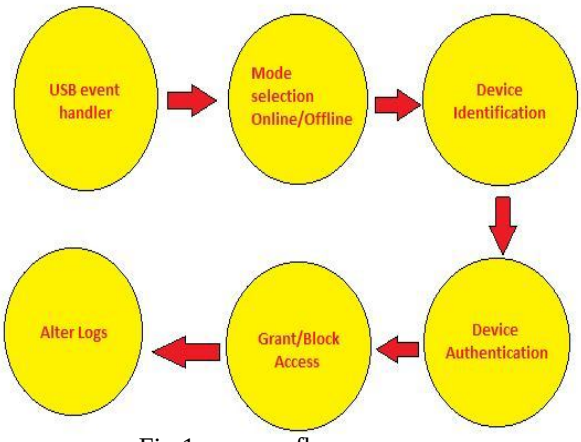


Fig 1: process flow

Following are the proposed algorithm for Data theft prevention & endpoint protection.

A. Device detection

Active the Thread Device =getNewDevice()

DeviceDescriptor d=getDeviceInfo() d.getdeviceId()
d.getVendorId()

B. Mode selection

1) Online detection: Online detection means workstation on which USB device plugged in is connected to network. In this case authentication and authorization will take place from online database [4].

2) Offline detection: This means workstation on which USB device plugged in is isolated or disconnected from network. In this case authentication and authorization will take place from local database maintained by the system [5]

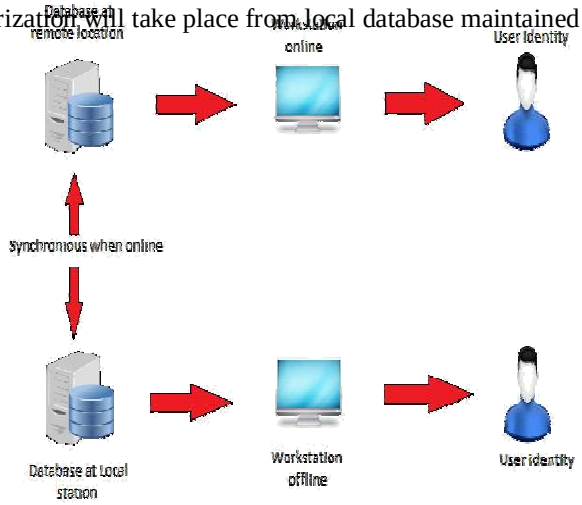


Fig 2: Mode selection.

C. Device Identification

Every USB device comprises a set of VID (Vendor ID) and PID (Product ID). These ID's are 4 characters hexadecimal ID; e.g. a typical VID looks like VID_xxxx and PID looks like PID_yyyy, where xxxx and yyyy are hexadecimal number.[6]

D. Device authentication

Devices are authenticated by a White list (a list of authorized USB devices) located on a remote server database. In online mode devices should authenticated directly from server white list.[4] If device is offline it should keep a local copy of remote white list in encrypted format to authenticate devices and maintain security. This

1) Authentication process is called 2-way authentication.

At this place we take decision to block \ allow USB device to communicate with workstation.[4]

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

B ←Authorize

else

B ←Un-Authorize Return **B**

E. Block/unblock device

Disable port=1
If B ← unauthorized
Disable port=true
Else
Disable port=false

F. Alter and log Input

VID: Vendor ID of USB Device
PID: Product ID of USB Device
Host Name: Get the host name of computer
Login ID: Get digital identity of user IP Address: Get IP address of computer
Output:
B: Successful/Un-Successful IF VID ≠ 0 and PID ≠ 0
B ← save log Send e-mail or SMS to the
alert
If B ==1 then
Return B ← Successful
Else
Return B ← Un-Successful

III. EMPLOYEE IDENTITY AND ACCESS MANAGEMENT

It refers to the management of identity, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and load on system.

In an organization there is many ways to authenticate an employee uniquely by employee id, full name, face etc., but in digital word same has been done by digital identity [3].

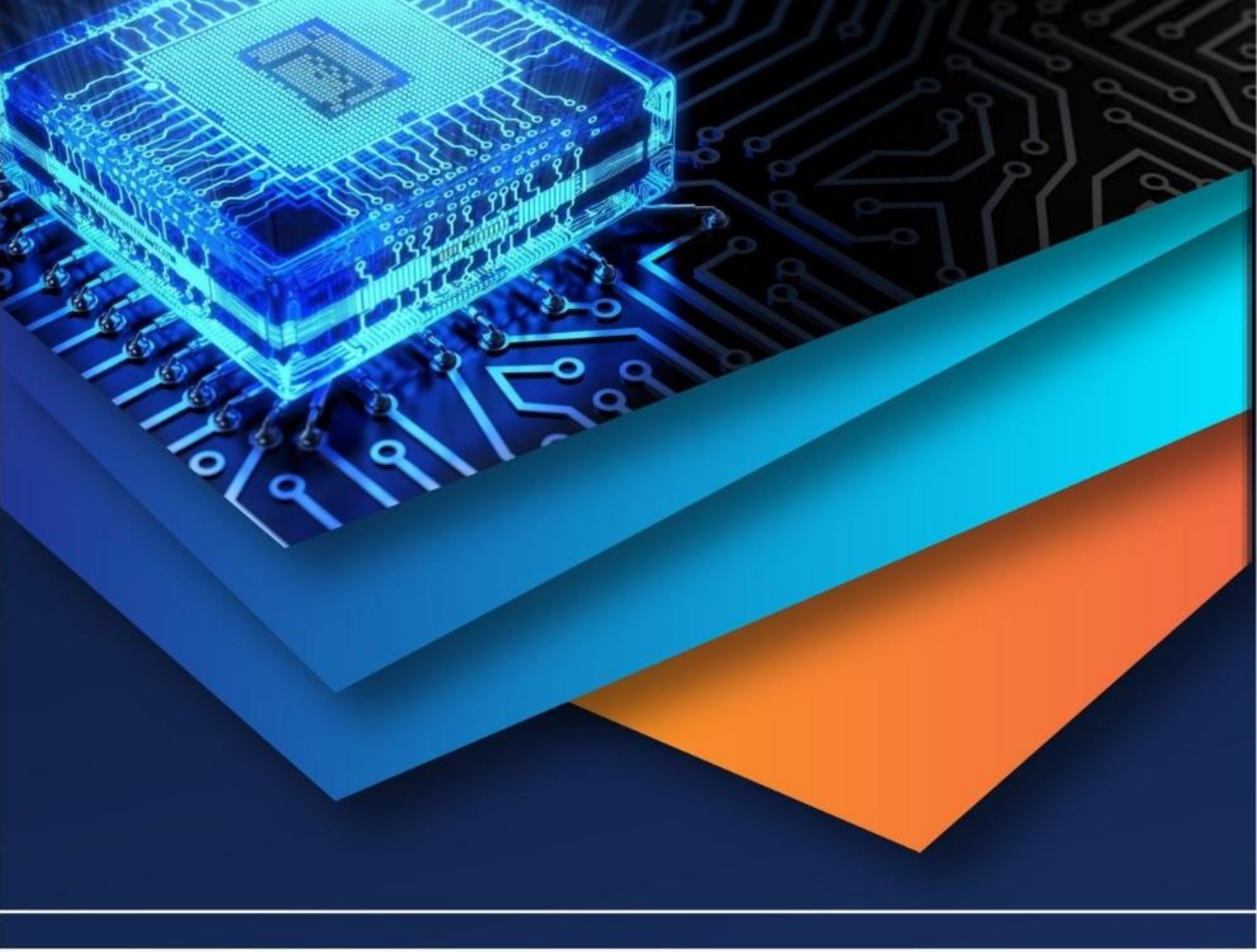
In our implementation we have logged all events. In logging information we have proposed to fetch all possible digital identities (e.g. entities' login ID, Host Name or serial number of workstation etc.) by which we can extract pattern of employee by which he plug in devices (Authorized \ Un-Authorized) and prevent data theft [1].

IV. ACKNOWLEDGEMENS

We would like to acknowledge and extend our heartfelt gratitude to the following persons who have made the completion of this application possible: Mr. Vineet Sharma (Scientific officer at Bhabha Atomic Reaserch Center(BARC)) and Mrs. Sneha Kolhe for their vital encouragement and support.

REFERENCES

[1] Saurabh Verma, Abhishek Singh, "Data theft prevention & end point protection from PnP Devices" ISBN: 978-93-81583-71-5, National Conference on Communication Technologies & its impact on Next Generation Computing 2012.
[2] Nikita Agwankar1, Dr. Sunil Surve2, Prof. Sapna Prabhu3, Radhika Nayak, "Security For Portable Data Storage media", ISSN (Print) : 2319-5940, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1, April 2013.
[3] Hui Pan, Editor; Paul Polishuk, Editor (April 1998). "Definition of Universal Serial Bus". 1394 Newsletter **2** (4): 7–9. Retrieved 2010-03-11.
[4] Julius Baer CEO, BAER.VX, "Client data theft" Reuter US edition, August 27 2012.
[5] Pham, D.V. "Threat analysis of portable hack tools from USB storage devices and protection solutions," IEEE ISBN: 978-1-4244-8001-2 [2010 International Conference on, vol., no., pp.1-5, 14-16 June 2010].
[6] Kami Makki, Md. Sadekur Rahman, "An Authentication Middleware for Prevention of Information Theft", ISSN: 2305-0012, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(3): 18-26 The Society of Digital Information and Wireless Communications, 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY