A SECURE DATA TRANSFER TECHNIQUE FOR USB DRIVE

[1]Mrunal P. Kene, [2]Nitin N. Mandaogade

[1]2nd Year M. tech in Electronics and Telecommunication Engineering,
[2]Associate Professor, Dept. of Electronics and Telecommunication Engineering,
G H Raisoni University Amravati, India.

Abstract : The primary motive of this system is to protect USB drives. A USB drive is a drive that transfers data at fastest verbal exchange velocity. In maximum cases, it is possible to lose information, because of a person can delete the facts and once in a while the USB may be stolen. The facts can be private or legitimate. If the information is stolen, facts may be misused, which means random human beings will misuse the records. The nuclear password or navy password is also stored in USB, and while an authenticated man or woman connects the power, simplest statistics may be retrieved. Therefore, it's miles quality to construct a device that doesn't allow get right of entry to information until the person profits get admission to rights. This paper will attention on who can protect USB drives through hardware. The great part of the system is that we are able to stop the information being transmitted on request. If the consumer is authenticated, simplest he/she can retrieve the statistics. To this quit, we're creating a system that is completely hardware-based and might transfer transistors. But the USB force is still stolen, the proprietor sends a predefined command to the USB force, after which it'll show the contemporary location.

***IndexTerms* - Flash drive, USB data blocking, By-directional SMS.**

I. INTRODUCTION

USB (Universal Serial Bus) garage devices are one of the most appropriate and popular to shifting records between unique computers. USB can be visible because the renewal for ZIP- drives, Floppy disk and all that type of media.

Miserably, there may be a possibility of information theft and records leakage. This can be minimized and overcome with cognizance, care and by the usage of correct gadgets or gear to comfy the facts.

As we all recognize, there are numerous software to ensure the safety of Pen-Drives software. In many universities or organizations, there are problems with USB, this means that it cannot be linked/unrecognized. In reality, this isn't a USB trouble, it could guard the laptop from such drives. However the safety of USB is still a large difficulty.

So far, all systems related to the implementation of USB safety are software-based totally. But this is a hardware-based system which can guard USB.

II. PROPOSED SYSTEM

A. Model Of The System

Below figure shows the model of system.

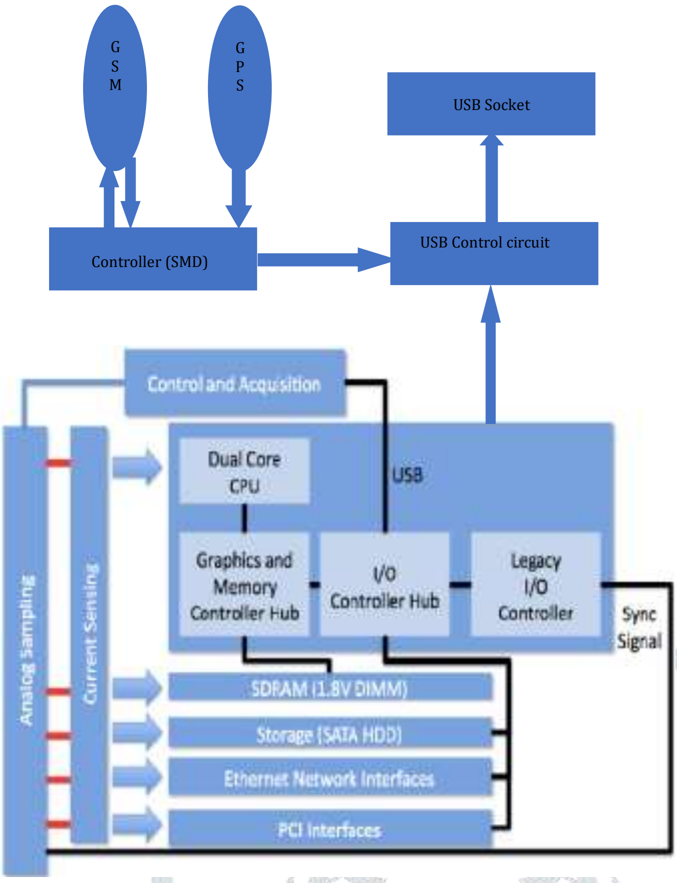

Fig.1- Model of the system

We are offering an embedded solution for USB security gadgets. In this solution, we have used the ATmega 328 microcontroller for embedded C programming, for region detection, GPS is used and GSM for sending and receiving SMS.

Each time a consumer wants to access his USB, as long because it starts operating, there's want to send a particular command to the USB. Secondly, if a person discovers that his USB tool is stolen at that point, the user wishes to ship a particular command to the system and the inner user will get the area of the USB force.

B. Block Diagram Of The System

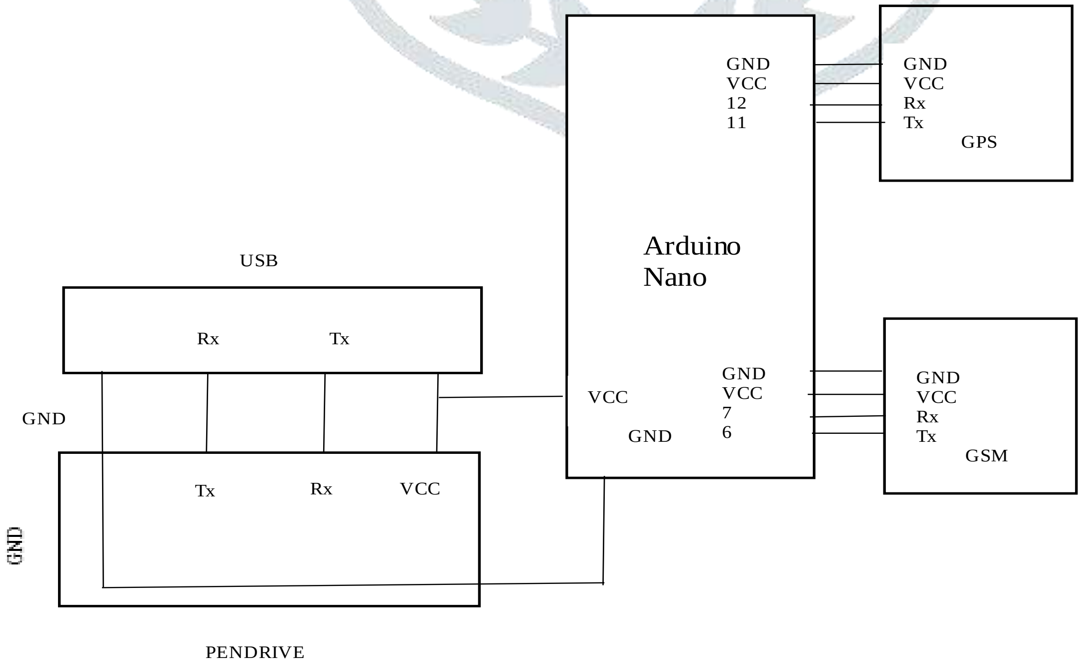

Fig.2- Block Diagram of the system

In our proposed system, we used one chip i.e. Microcontroller ATmega328 which is a low power CMOS 8 bit Microcontroller.

The figure 2 shows the USB driving force and control circuit, where GPS and GSM work one at a time. Each GPS and GSM send their readings to the controller SMD. Here, we're using the ATMEGA 328 controller, that is the centre of the system.

Whilst we connect Pen-Drive to the device, the controller will switch on. Now, we have to ship a predefined command including "ON", and then this message can be dispatched to the controller through GSM. The controller will take a look at the command with the assist of programming. If the command matches with the predefined command, most effective the information consumer can get entry to the facts. Otherwise, USB will no longer allow unauthorized employees to get right of entry to it.

C. Progression Work Diagram

Below diagram is for secure data transfer technique for USB drive.

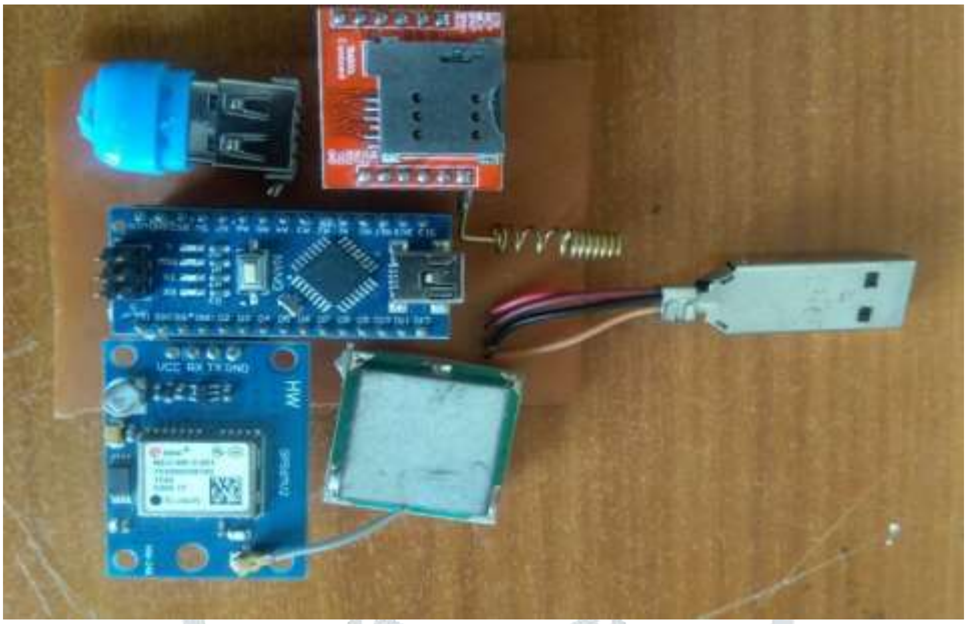

Fig.3- USB Security system

USB control circuit is totally transistor based circuit. With the help of transistor switching we will ON or OFF the Pen-Drive at unique time. Information is transferred consistent with the speed of transistor switching.

We've got visible a couple of instances, with the help of transistor switching LED receives ON or OFF as well as buzzer gets ON or OFF however we've got in no way seen that transistor can prevent the statistics.

While the base is active, emitter shots with collector i.e. data came via collector and is passes through emitter means if it go to the depletion layer then there may be a probabilities of deleting the records or records hacking.

III. Advantages Of The System

- Stop data access by unauthorized person
- Block pen drives anytime, anywhere
- A self-powered system, even if an unauthorized person is not using it, also be used to detect the location of the pen drive.
- Embedded integrated system will respond to user's praise for using SMS
- Make the device compact and light, use it as an extension of a normal pen drive without increasing its size
- If someone uses the pen drive without authorization, it will track its location.

IV. Applications Of The System

- This project will help to secure USB drive from unauthorized data collectors
- This system will help to find lost drives

V. Result

At the beginning, our system isn't in operating mode i.e. it is in off state. Whilst we connect Pen-Drive to system, controller will ON automatically. After that we ought to ship a selected command like "ON", then this message is going to a controller through GSM. Controller will test the command/message with predefined command. If the command suits with the predefined command, most effective the information user can get right of entry to the information. Otherwise, USB will no longer allow unauthorized personnel to get admission to it.

If the USB is stolen then we need to enter command like "FIND", then with the assist of GPS we are able to tune/track the place.

VI. Conclusion

In this article, an idea of finding a Pen-Drive is proposed and designed with the help of a circuit, and the belief of the circuit is proven in the MATLAB Simulink model. The version offers the result and adds it to the GPS. The barcode feature makes it easy to locate any object. With the assist of this device, we will prevent statistics/Pen-Drives from being stolen or misused.

References

[1] Mrunal P. Kene, Nitin N. Mandaogade "USB Drive Security System : A Review", International Research Journal of Modernization in Engineering Technology & Science, vol:03/ Issue:03 March 2021 from https://irjmets.com/rootaccess/forms/uploads/IRJMETS870680.pdf

[2] V. S. Kumbhar, S. K. Kharade, K.G. Kharade, "Setting barrier to removable drive through password protection for data security", International conference on "Innovations in IT and management", vol:68, special issue-27 February 2020.

[3] Rishabh Srivastava, Abhishek Jain, Shradha Porwal, "Pen-Drive security based system", 3rd International Conference on Internet of things and connected technologies", issue:2018 https://www.ssrn.com/link/3rd-ICIOTCT-2018.html

[4] Kyungroul Lee, Insu Lee, Yeunsu Lee, Hyeji Lee, Kangbin Yim, Jungtaek Seo, "A study on secure USB mechanism that prevents the exposure of authentication information for smart human care services", Journal of sensors, special issue: 29 October 2018.

[5] J. Clark, S. Leblanc, and S. Knight, "Hardware trojan horse device based on unintended USB channels," in 3rd International Conference on Network and System Security. IEEE Computer Society, May 20019, pp.1–8.

[6] Hung Cheng Chen, (Us); Keng Hao Chang(Us), "Object Finder", Patent Application Publication, March 14 2013, Publication No. Us 20130063261 A1, Date of access: 29/1/2014

[7] J. Clark, "On unintended USB channels," Masc. Thesis, Royal Military College of Canada, Feb. 2018.

[8] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware trojan design and implementation," in IEEE Intl. Workshop. on Hardware-Oriented Security and Trust - HOST'09. IEEE Computer Society, Jul. 2019, pp. 50–57.

[9] T. S. Chou and J. W. S. Liu, Fellow, IEEE," Design and Implementation of RFID- Based Object Locator", Institute of Information Science, Academia Sinica, November 2007, Technical Report No. TR-IIS-06- 014, Date of access: 29/1/2014

[10] Sinan Adnan Diwan, Dr. Sundresan Perumal, Ammar J. Fatah "Complete security package for USB thumb drive", computer engineering & intelligent system, vol.5, No.8,2014.

[11] Hanjae Jeong, Yunho Lee, Seungjoo Kim, Dongho Won, "Vulnerabilities analysis of secure USB flash drive", Information security group, Sungkyunkwan University.

[12] "Compromise through USB-based hardware trojan horse device," Future Generation Computer Systems, vol. In Press, Accepted Manuscript, pp. –, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/B6V06 - 4YXP15K - 4/2/6726e8fde4fc1476f895f6edd0657e99

[13] Jim Louderback, "Computer crime, vulnerabilities of information system and managing risks of technology vulnerabilities". Ridgetop Information Solution LLC Charmayne cullom, Ph.D. Published in USA weekend August 10-12-2001. www.profhelp.com

[14] Mr. A. N. Magdum, Dr. Y. N. Patil "A secure data transfer algorithm for USB mass storage devices to protect documents", in International Journal of Engineering Research & Technology, vol:2, issue:4 July 2014.

[15] "USB Device Class Definition for Audio Devices 2.0," 2018, http://www.usb.org/developers/devclass/docs/Audio2.0/final.zip.

[16] Larry Hamid "Biometric technology: not a password replacement, but a complement", Biometric technology today, June 2015.

[17] Keun-Gi Lee, Hye-Won Lee, Chang Wook Park, Sangjin Lee "secure USB thumb drive forensic toolkit", International conference on Future generation communications and networking.

[18] Sun-Ho Lee, Kang-Bin Yim, Im-Yoeng Lee, "A secure solution for USB flash drives using FAT file system structure", International conference on Network – Based information system, issue 2010.

[19] Jaein Kim, Taeyoung Jung, Dmitry Volokhov , Kyungroul Lee "Vulnerability to flash controller for secure USB drive", Journal of Internet Services and Information Security(JISIS), vol:3, No.3/4.

[20] R. Arvind, R. Lavanya, M. Senthil Kumar "The Computerized Pen-Drive" in International journal of computer applications, vol 41,No5,March2012. From http://www.brevard.k12.fl.us/infosec/documents/SevenStepstoSecureUSBDrives .pdf 5

[21] Debiao He, Neeraj Kumar, Jong-Hyouk IEEE Transactions on consumer Electronics, vol 60, No. 1 February 2014.

[22] Portable Panic, The Evolution of USB Insecurity, Retrieved from http://www.preventia.co.uk/resources/white_papers/lumension/the-Evolution-of-USBInsecurity.pdf 7

[23] Senforce Technologies. (January 2007). Best Practices for Managing and Enforcing USB Security: Five Questions You Should Ask About USB security from http://www.pcsltd.com/pdf/012007-USBWhitepaper.pdf 8

[24] Steve Wiseman. (April 2006). Retrieved from http://www.intelliadmin.com/index.php/2006/04/disable-usb-drives/ 9. Techmirchi. (2013).Retrieved from http://techmirchi.com/how-to-password-protect-usb-drivewithout-using-software/

[25] University of Maryland Department of Criminology and Criminal Justice Fall. (2004). Computer Crime and Computer Fraud, Retrieved from http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf 12.

[26] Watson, Los Angeles Times. (April 2006). 'US military secrets for sale at Afghanistan bazaar'.

[27] R. Tulasi, K. Ravi Kiran "Security protocol for USB mass storage devices" in International research journal of engineering and technology, volume:03,issue:01Jan2016.

[28] Ketan Kakade, Darshan Marode " Secure file transfer using USB" in International journal of scientific and research publication , vol 2,Issue 4,April2012.

[29] Hanjeejeong, Yunho Lee, Seungjoo Kim, Dongho Won"Vulnerability analysis of secure USB flash drive" Information security group, Sungkyunkwan University,IEEE Xplore,January 2008.

[30] Bianca Gallo Pucci, Donald Pucci," Radio Frequency Object Locator System", Patent Application Publication, May 16 2013, Patent No. Us 7046141 B2, Date of access: 26/1/2014

[31] USB Implementers Forum, "USB device class definition for human interface devices (hid) 1.11," 2017, http://www.usb.org/developers/devclassdocs/HID1

[32] "USB HID usage tables 1.12," 20019, http://www.usb.org/developers/devclass docs/Hut1

[33]Microsoft, "Windows Media: WAVEFORMATEXTENSIBLE," 20018, http://msdn.microsoft.com/en-us/library/aa391547(VS.85).aspx.

[34] USB Implementers Forum, "USB device class definition for mass storage class - control/bulk/interrupt transport 1.11," 2019, http:// www.usb.org/developers/devclass docs/USB msc cbi

[35] Computer Crime, Vulnerabilities of Information Systems, and Managing Risks of Technology Vulnerabilities, Retrieved from http://www.profhelp.com/crime/computercrime.pdf