Security System For Pen Drive

Shubhangi N. Ghule[1], Aishwarya A. Bhujbal[2], Arati M. Gunaware[3], Mrs. Shilpa S. Kanse[4]
[1, 2, 3, 4] Department of Electronics and telecommunication Engineering
[1, 2, 3, 4] RSCOE, Pune

Abstract- *USB is generally use to transfer data between two devices by using controller and PC. But it is not always possible to secure data of USB once it is stolen, so to overcome this problem, we are designing a fingerprint based biometric pen drive system so that can data can be secure. This device is connected to a PC over USB, and using application-layer software on PC, it allows the user to read and store data on the device. 10 fingerprints can be stored on the device, and each fingerprint has a separate location so that the user can utilized as their own specific storage space.*

Keywords- Fingerprint module, SD card, USB, Keypad.

I. INTRODUCTION

Till date transmission of data is carried out using different protocols like- USB cables, pen drives etc. [1]. These are efficient wired data transfer techniques but data can also be transferred wirelessly [1]. This will help us to reduce the hardware requirement. Also it will reduce the complexity. Another major concern is data security and privacy.

Due to advance use of removable devices for data storage and data transfer, so maintaining confidentiality is essential. Due to this, the usage of these devices are tremendously increased. It also possess huge risk of data being compromised and being misused. Therefore, Despite their convenience and ease of usage, removable devices (USB) have been prohibited in most of the institutes/organizations [2]. But preventing or reducing the usage of these devices is not a valid solution. USB's usually store different kinds of important data. The Finger print based Biometric Access Controls USB Flash Drive, USB key for secure storage of the data and applications

II. LITERATURE SURVEY

- Authors G. Gowsica and L. Latha described that Finger Vein is a method of biometric authentication. It uses pattern recognition techniques [7]. It matches the vascular pattern in an individual's finger to previously obtained data.
- Authors Jasmin Jivani, Samuel Johnson, Gayatri Pandi Presented that there are two Cryptography encryption techniques are used [2]. These are symmetric and asymmetric encryption techniques. AES, DES, IDEA are examples of Symmetric encryption algorithms. RSA and DSA algorithms are come under the Asymmetric encryption.
- Author Jan Axelson provided details for anyone working with USB for any purpose [5]. It is used for designing a peripheral or creating a host software.
- Kaustubh Gaikwad, Sneha Ojha, Shreyas Surlikar Supriya Zende described how the pen drive is created by using controller, SD card and flash drive [1]. Also, we came to know about how to transmit the data between PC and pen drive.

III. BLOCK DIAGRAM OF SYSTEM

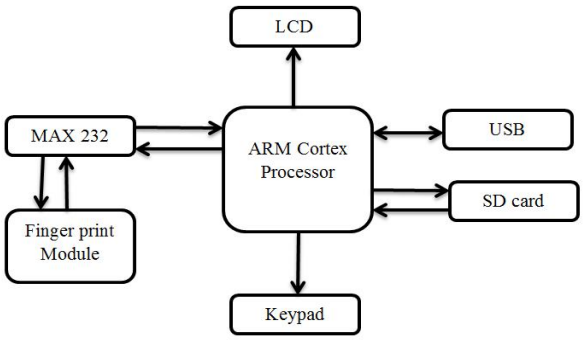

Figure 1. block diagram

1. ARM CORTEX LPC 1768

- It allows high level of integration and low power consumption.
- Required 512 KB of flash memory.
- 64 KB of SRAM
- 8 channel general purpose DMA controller
- 4 UARTs, 2 CAN channels, 2 SSP controllers, SPI interface, 3 I2C interfaces.
- 8 channel 12-bit ADC, 10-bit DAC.
- 4 general purpose timers, 100 pin LQFP package
- 4 power modes (sleep, deep sleep, power down, deep power down mode)

Figure 2. fingerprint module

2. FINGERPRINT MODULE

- Integrated image collecting and algorithm
- chip together.
- Low power consumption, low cost, small size, excellent performance.
- Good image capturing capabilities, can successfully capture image up to resolution 500 dpi.

Figure 3. Finger print module

3. SD CARD

Figure 4. SD card

- Secure Digital (SD) is a non-volatile memory card format developed by the SD Card Association (SDA) for use in portable device.
- SD Standard Capacity: Capacities for SDSC cards range from 128 megabytes to 2 GB. The default format for these cards is FAT16.
- SD High Capacity:z Based on the SDA 2.0 specification, capacities for SDHC cards range from 4 GB to 32 GB. The default format for these cards is FAT32.
- SD extended Capacity: Based on the SDA 3.0 specification, SDXC range from 64 GB to 2 terabytes. The default format for these cards is exFAT (Extended FAT).
- SD Input Output:- SDIO cards combine I/O functions with data storage. As of 2016, the SD Card formats are full or micro-size SDHC and SDXC cards.

4. USB

Universal Serial Bus, USB is a plug-and-play interface that allows a computer to communicate with peripheral and other devices.

- Serial communication.
- Two way communication between PC and peripheral devices.
- Hot swappable.
- Multiple devices can be connect.

Figure 5. USB

SOFTWARE REQUIRED:

- The µVision IDE KEIL4 combines project management, run-time environment, build facilities, source code editing, and program debugging in a single powerful environment.
- Flash Magic is a PC tool programming flash based microcontrollers from NXP using a serial or Ethernet protocol while in the target hardware.
- Proteus is used for simulation and PCB layout.

IV. FLOW OF WORKING

- Power on
- Microcontroller initialization
- LCD Display
    1. Admin
    2. Unlock

In Admin there are two options.

- Add
- Delete

If you want to register fingerprint then press 1 on keypad. Enter the two digit location with help of keypad. Put a finger on fingerprint module. Within 5 seconds Fingerprint

will successfully register. You can delete this registration by delete option in admin.

- In unlock you can verify your fingerprints. Press enter on put a finger. If fingerprints are matched then LCD will display user found.
- After verifying user's fingerprint data lines of USB initializes and pen drive will unlock.

V. EXPERIMENTAL PART

In this section, we present our solution in the form of a hardware device that meets the objective.

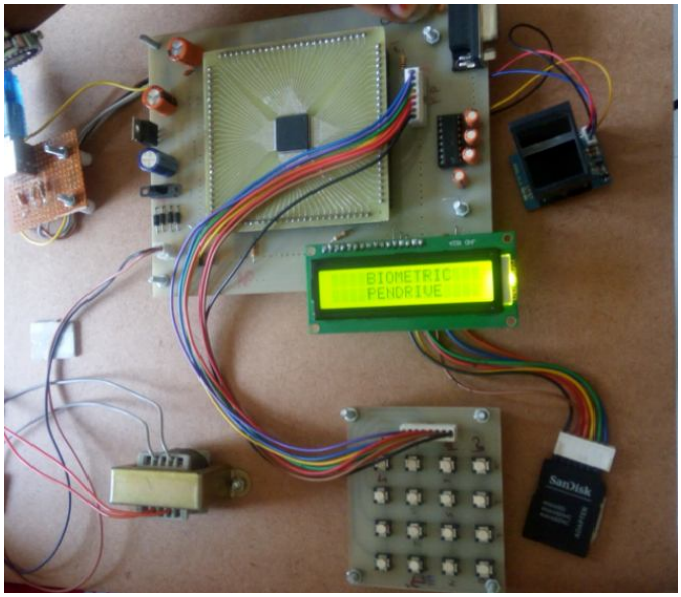

Figure 6. Snapshot of hardware

RESULTS:

This system shows 90% accuracy. Inaccuracy occurs because sometimes finger veins are not properly captured by the fingerprint module.

VI. FUTURE SCOPE

Along with the specified features the additional features that maybe added may include multiple user access, touchscreen in place of keypad and Wi-Fi network for security [1]. Security can be provided to the USB by the Wi-Fi network.

VII. CONCLUSION

In this paper main focus is on the security of pen drive using fingerprint authenticated system. This design provides security to the pen drive for the users against data theft. Data will secure even if pen drive is stolen. Except user nobody will able to unlock the pen drive. The Finger print based Biometric Access Controls USB Flash Drive. It gives fingerprint access control to the content of the USB key for secure storage of the data and applications [2]. Communication between PC and fingerprint module for identification of user is effectively studied.

REFERENCES

[1] BIOMETRIC WIRELESS PEN DRIVE (IRJET)

[2] A Review of USB Encryption Techniques & Algorithms for Data Confidentiality

[3] www.ijarcsse.com

[4] http://fingerprint-it.blogspot.com

[5] USB complete: Everything you need to develop USB peripherals, Third Edition by Jan Axelson.

[6] International Journal of Advanced Science and Technology Vol. 4, March, 2009, A Brief Introduction of Biometrics and Fingerprint Payment

[7] A Survey on Biometric Authentication Techniques