WIRELESS BIOMETRIC DATA PROTECTION IN PENDRIVE

Dr. G. NARMADHA [1], S. DEIVASIGAMANI[2], S.SIVAGURU[3]
1. Assistant professor, Sethu Institute of Technology, Virudhunagar, India, gnarmadhame@gmail.com
2. Senior Lecturer, Faculty of Engineering and Computer Technology, AIMST University, Malaysia, deivasigamani@aimst.edu.my
3. Research Scholar, Faculty of Information, Science&Technology, UKM, Malaysia, shivguru@yahoo.com
4. Manickam Ramasamy, Lecturer, Faculty of Engineering, Technology & Built Environment, UCSI University, manicks36@gmail.com

Abstract— **Recently the data is protected by using external disc like USB flash drive in normal binary format. Pen drive is the most popular device because of its size, low cost, large storage capacity and relatively high transfer speed. If it is stolen/missed somewhere, one can easily retrieve the personal information stored in it. So the main intention of the proposed methodology is to provide the data confidentiality in using the pen drive and it will be used in a more secured manner with the limited cost. Authentication is achieved by using the biometric system. The pendrive can be accessed only with the help of the user's finger print. This concept can be used where the high data authentication and device security is needed.**

Keywords: Fingerprint sensor, SD card, wireless module, Wifi security.

1. INTRODUCTION

Biometrics is the technological term of the human body dimensions and calculations. It refers to metrics related to the features of a human. Realistic authentication is used in workstation for identification and access control. It can also be used to recognize individuals in groups which are under supervision.

Biometric identifiers are the typical, assessable characteristics which are used to find and depict the characteristics of individuals. These are classified in to physiological and behavioural characteristics. Physiological characteristics deal with the shape of the body. It includes palm veins, fingerprint, DNA, face recognition, hand geometry, palm print, iris recognition, odour/scent and retina. Behavioural characteristics depend on the pattern of behaviour of an individual which includes voice, typing rhythm and gait.

The conventional means of access control are the token-based identification systems which includes driver's license or passport, and knowledge-based identification systems like personal identification number or password.

Biometric identifiers are more reliable then knowledge and token based methods because of its uniqueness among individuals and identity verification ; however, the compilation of biometric identifiers raise privacy concern for the vital use of the data.

1.1 FUNCTIONALITY

Several aspects of human physiology, behaviour or chemistry can be used for biometric authentication. The choice of a specific biometric for particular application depends on the weighting of various factors. Jain *et al.* (1999) [7] recognized seven factors which are used to assess the suitability of any kind of trait to be used in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

The specific choice of biometric depends mainly on the application. Some biometrics results in better performance than the others while considering the security and flexibility. Any biometric will not satisfy all the requirements of particular application.

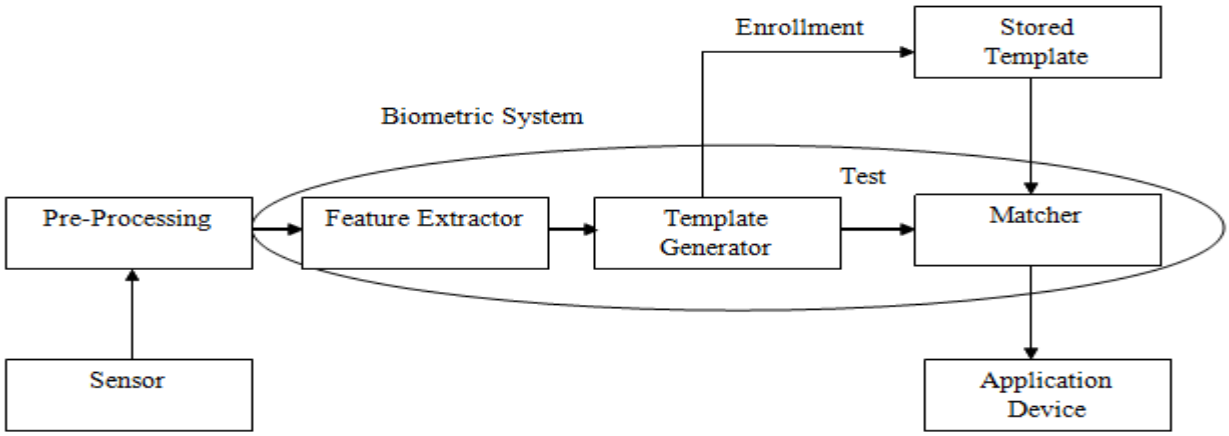

Figure 1. Block Diagram of Biometric System

The block diagram of biometric system is shown in the Figure 1 and it shows the two fundamental modes of a biometric system. First mode is the verification mode and in this mode, a one-to-one assessment is performed on the captured biometric with a particular template which is already stored in a biometric database for verifying the person who are under claim. Verification of a person involves three steps. In step 1, reference models are generated for all the users and are stored as the model database. In step 2, threshold is calculated by matching some samples with reference models in order to generate the genuine scores. Testing is the third step. Usually, PIN or ID number, smart card are used for comparison.

Second mode is the identification mode and in this mode, a one-to-many comparison is performed against a biometric database to find the identity of an anonymous person. The system will get the positive result if the comparison result of an individual and the biometric sample of the template in the database come under the preset threshold. This mode can be used for either positive recognition (information about the template to be used is not necessary) or for negative recognition of an individual (it establishes whether the person is implicitly or explicitly denied). It can be achieved only through biometrics when the other methods such as PINs or keys, passwords of personal detection are ineffective.

The human body has the exceptional features that are unique and limited for each and every individual. Because of this uniqueness and exclusive characteristic, various embedded computers and controllers have been entered in the field of biometrics for ensuring authentication in several fields.

Biometrics has gained recognition and proved itself to be a consistent mode of ensuring confidentiality, maintaining security and identification of the individuals. It has been accepted by throughout the world and is used at various places like corporate offices, hospitals, airports, colleges, schools, etc. Biometrics is the study of identifying an individual based on their physical traits that are inborn and unique to each and every person. Biometric identification includes palm geometry, fingerprint verification, iris recognition, face recognition, etc. These techniques work at the different levels of accuracy and functionality. The most essential parameters in the biometric applications with the embedded computers are reliability and accuracy. The commonly used biometric technique is the fingerprint verification due to its simplicity and better levels of accuracy. It is known fact that each and every human is born with a different finger pattern and this feature is subjugated to recognize and differentiate the two different persons and it is the factor which is used to instigate the model .

Up to date, it is known that USB is universally accepted teeming interface, normally used for transferring data from one device to another etc.. This interface gives several pros. but it has some cons. such as 1] illegal person can easily disclose the confidential information in which the data stored in the “plain text” format. 2] An attacker/hacker can easily hack the information transferred between the devices and computer over a bus or a channel which is open(eg. Virus/malware). To avoid this kind of malware a fingerprint authenticated wireless pendrive is designed. Only authorized person can able to access the data stored in the SD card. To use the SD card, a user simply authenticate by placing his/her thumb/middle finger on the fingerprint sensor.

The desired data to be transmitted is selected from the SD card using a keypad and LCD which are interfaced with Arduino module. LCD is interfaced to display the data present in the device. The Keypad is interfaced for selecting the contents present on the SD card so that data can be transferred. Arduino provides an interface between the input devices and Wi-Fi module. On the receiver end the PC or laptop is connected to the Wi-Fi and thus data is received and displayed.

1.2 ISSUES AND CONCERNS

1) Human dignity

The human subject is turned into a collection of biometric parameters, it would dehumanize the person, violate bodily honour and eventually, insult human dignity. Sometimes, it will cause damage to the owners also.

2) Cancelable biometrics

The advantage of using passwords instead of biometrics is that the passwords can be re-issued. If a password is stolen, it can be made invalid and replaced with a newer password. This method is not naturally possible in biometrics. If a person's face is compromised from a database, they cannot be cancelled or reissued. If the biometric identifier is stolen, it is impossible to replace a biometric feature. Cancelable biometrics is an approach to integrate protection and the substitution features into biometrics in order to build a more secure system.

3) Soft biometrics

Soft biometrics traits are behavioural or physical characteristics of a human that have been derived from the way in which they differ from others (e.g. gender, height, hair color). They are used to harmonize the uniqueness information given by the primary biometric identifiers. The soft biometric characteristics require the distinctiveness and durability to identify an individual reliably and uniquely and can be faked easily, they offer some proof about the users identity that are beneficial. Combinations of human attributes like race, gender, height , eye color and other visible identification parameters are used to improve the concert of traditional biometric systems. Soft biometrics can be collected easily through enrollment. Soft biometrics have two main ethical issues. First, the soft biometric traits are sturdily cultural based. Second, soft biometrics have strong potential for profiling and categorizing people, so the processes of exclusion and stigmatization are supported at high risk.

Section 2 describes the existing work with the biometrics. Section 3 depicts the implementation method. Experimental setup is explained in Section 4. This paper is concluded in Section 5 and the future scope is illustrated in the Section 6.

2. LITERATURE SURVEY

The high data transfer rate, high availability, and ease of connectivity are main advantages of handy storage device. Conversely, at an application level, the handy storage devices suffer from major security weaknesses [1], an unauthorized user can easily read or steal secret information as it is stored in plain text form, and an attacker can capture all the information which have sent over the bus between the device and the USB port of host computer which can be opened to the attacker (e.g. physical, virus or malware). User authentication and session key agreement are designed in such a way that they can resolve the aforementioned difficulties. Carrying a laptop or computer is just for the sake of data transfer and is not reasonable. In these days, the aged people want all devices to be versatile. Moreover, transferring data through a computer involves a set of power to be exhausted, because the computer has to be functioned entirely during the data transfer. Also, the threat of malware and viruses has reduce the efficiency of computer [2]. When the device is plugged in to the system for data transfer, these viruses are activated and transferred along with the data to the another device in which it is plugged.

From above two papers they used the text code as a password protected portable storage device and data transmission between the USB to USB without using computer so still there exits problems, such as the passwords can be decrypted using different software. A Pen drive or SD card is used to store important data in an unencrypted binary format. This device is very popular due to its size, large storage capacity and relatively high data transfer speed. But, if the device is lost or stolen all the information can be easily accessible so biometric systems are used to identify, verify and gives authenticated access control to human by comparing their behavioral and physiological characteristics with the enrolled data [3].The Biometric Wireless Pen drive is almost same as that of normal USB Flash Devices but some additional features are added to support the Wireless data transmission and reception [4]. Wireless USB enables PC peripherals and point-to-point or multipoint-to-point applications [6] with the ability to replace the USB wire with a low-cost, 2.4-GHz wireless solution [5].

Finally in this proposed system, the three methods are combined and are listed below to solve the problem of data security and also data transmission.

A. Biometric Authenticated Security System using fingerprint sensor module.

B. Wireless communication for data transmission using Zigbee module.

C. Wireless charging unit.

3. IMPLEMENTATION

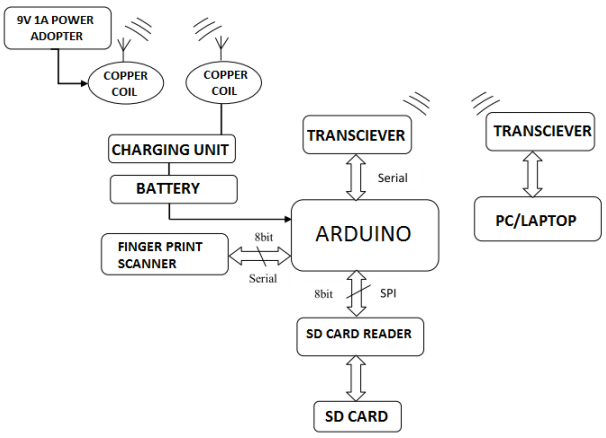

Figure 2. System Block Diagram

3.1 WORKING DESCRIPTION

The proposed model shown in the Figure 2 consists of the Fingerprint Scanner, SD Card Reader/Writer, SD card, Wireless Communication (Zigbee cc2500), Inductive Charging Unit, Power Supply and Lithium Polymer battery.

Fingerprint Scanner (R303): Fingerprint sensor (R303) is required for authentication which is used to identify the storage device. In this module, up to 120 fingerprints can be stored with diverse address location in flash library.

SD Card Reader/Writer: This reader contains 5 pins which is used to read and write the contents from the storage device.

SD card: This is used to save the data files and 2Gigabytes data storage device is used in this module.

Wireless Communication (Zigbee cc2500): This is essential to transmit or receive the data between the USB device which is authenticated and computer/mobile through wirelessly. It works with the frequency range of 2.4GHz.

Inductive Charging Unit: This unit is used for the wireless charging in the proposed system.

Power Supply: This is required to simulate the input power source to the induction charging unit that charges the battery, while demonstration of the developed project.

Lithium Polymer battery: A suitable specification battery which is used to store the energy from Inductive power supply.

In proposed system, first the user has to authenticate by placing his finger on the fingerprint scanner, if finger print matches with stored image, then user can read/write data to the SD card. If doesn't matches then the access to SD card is denied. Here Zigbee transceiver is used for the wireless data transmission between the proposed model to personal computer/laptop. Along with all these things, the wireless charger is included for the portable application purpose.

3.2 Fingerprint Module

The surface of a human finger has a series of ridges and furrows and it also has a core which is enclosed by unique patterns of loops, swirls and arches which compose the fingerprint of each and every individual unique. By using this characteristic of a human finger, the fingerprint modules get activated and is shown in the Figure 3.

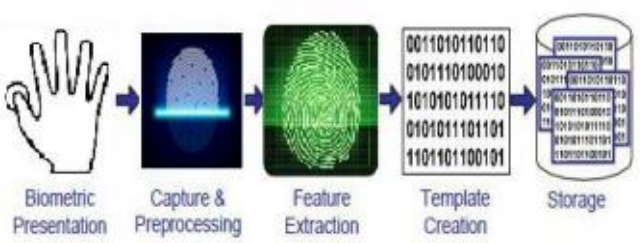

Figure 3. Scanning Process

There are five stages in the scanning process. They are 1-Biometric Presentation, 2-Capture & Preprocessing, 3-Feature Extraction, 4-Template Creation and 5-Storage.

The fingerprint scanner takes a snapshot of the user's fingerprint. The captured fingerprint is preprocessed and a code is generated based on the features extracted from the finger which are different for every user. The code generated is stored in the Arduino. Every time the user accesses the SD card, the fingerprint authentication is required and the access is granted only when the scanned fingerprint matches with the enrolled fingerprint code.

3.3 WI-FI MODULE

Data will be transferred from sd card to PC/Laptop via Wi-Fi module MSP8266.This module is based on the 802.11 b/g/n standard and operates at 2.4 GHz with WPA/WPA2 security. Standby power consumption of < 1.0mW is achieved through (DTIM3) +20 dBm output power in 802.11b mode.

3.4 RECEIVER BLOCK DIAGRAM

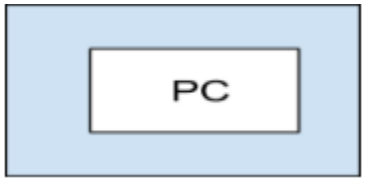

Figure 4. Receiver block diagram

Wi-Fi connectivity is required for receiving the data on the PC/laptop and is shown in the Figure 4. By using the HTML coding, the received data is displayed and stored. This text is not only received but it can also be retrived back into the SD card. There are no further hardware requirements or any changes required in the existing PC or laptop.

3.5. FLOW OF WORKING

Initially, a user places his/her thumb on the Fingerprint module which is used to verify the authenticated user. The module has an inbuilt ARM7 controller, which is further used to convert a fingerprint image into a corresponding code. This code will be compared with the previously enrolled user's code which is stored in Arduino. If both the codes match the user is given access to the SD card where the data to be transferred is stored. The file which is stored in the SD card will be displayed on the LCD, this enables the user to view the files and select the desired files using the keypad. Selected file can be sent through Wi-Fi module using the intranet. This sent file will be received on the PC/laptop as long as it is connected to the Wi-Fi

4. EXPERIMENTAL PART

In this section, the entire module is assembled and implemented in the form of a hardware device that meets the objective.

The entire prototype is shown in the Figure 5. In this module, the user's finger print is stored first for authentication and it is implemented by using arduino processor. The proposed module is tested by inserting in to the processor without the user's finger print and it is not accessed. With the user's finger print, the pen drive gets activated.

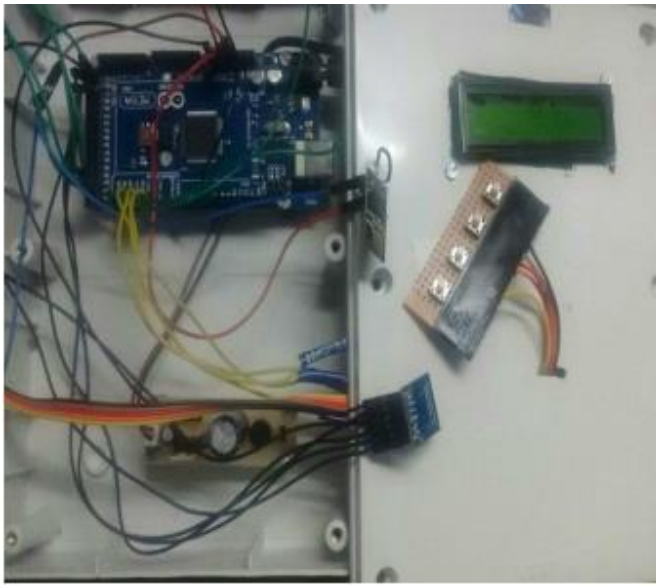

Figure 5. Experimental Setup

5. CONCLUSION

In this paper, focus is given on creating a pen drive which is completely secure, reliable and is able to send data wirelessly via Wi-Fi. Additional features like Biometric sensor, LCD display, keypad and controller will provide security, manage the concept behind the proposal which describes how to send and receive data from a pen drive to PC or laptop without using the USB ports of PC. The user can access the pen drive by placing it at some distance from the PC or laptop. The proposed biometric based wireless pen drive provides the data security and also the hardware security to the user.

6. FUTURE SCOPE

Along with the specified features, multiple user access can also be provided. Also the fine tuning can be done to improve the accuracy of the system and it can be developed for real time higher end application. Recently, mobile gets activated by recognizing the face of the user and by realizing the finger print of the user. Likewise, the pen drive is made to be accessed through the wrist watches.

REFERENCES

(1) Wei-Chi Ku and Shuai-Min Chen "Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY 2004.

(2) Mr.V.S.Gawali and Mr.A.M.Agarkar " Pen Drive to Pen Drive and Mobile Data Transfer Using ARM".Shegaon, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).

(3) Mr. M. Loganathan, Narendran, Rajeshkumar" Wired and Wireless Transmission of Data between Pen drives and Pen drives to Computer Using ARM" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-may 2014.

(4) USB Complete Everything You Need to Develop Custom USB Peripherals Third Edition, Jan Axelson.

(5) S. Y. Hui, Fellow IEEE. Planar Wireless Charging Technology for Portable Electronic Products and Qi, Proceedings of the IEEE | Vol. 101, No. 6, June 2013.

(6) Bradley Dietrich, san Francisco, Daniel Putterman, San Francisco, Gregory peters, Los Gatos," Methods and apparatus for transferring media across network using a network interface device" United States Patent, Apr. 19, 2011.

(7) Anil K. Jain, Salil Prabhakar, Shaoyun Chen, "Combining multiple matchers for a high security Fingerprint verification system", Pattern Recognition Letters 20 (1999), pp. 1371 - 1379